

User's Guide



Xirrus Management System

May 4, 2011
Release 5.1



Xirrus Management System

XMS 5.1

All rights reserved. This document may not be reproduced or disclosed in whole or in part by any means without the written consent of Xirrus, Inc.

Part Number: 800-0007-002
(Revision B)



Trademarks

XIRRUS is a registered trademark of Xirrus, Inc. All other trademarks and brand names are marks of their respective holders.

Notices

NOTE: These notices apply to XM-3300/XM-3320/XM-3340/XM-3360 Management Appliances.

FCC Notice

This device complies with Part 15 of the FCC Rules, with operation subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause unwanted operation.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate RF energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following safety measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Consult the dealer or an experienced wireless technician for help.

Use of a shielded twisted pair (STP) cable must be used for all Ethernet connections in order to comply with EMC requirements.

Non-Modification Statement

Unauthorized changes or modifications to the device are not permitted. Use only the supplied internal antenna, or external antennas supplied by the manufacturer. Modifications to the device will void the warranty and may violate FCC regulations. Please go to the Xirrus Web site for a list of all approved antennas.

Indoor Use Only

This product has been designed for indoor use only.

No Serviceable Parts

The XM-3300/XM-3320/XM-3340/XM-3360's enclosure must **not** be opened under any circumstances. This product contains no serviceable parts inside.

Safety Warnings

NOTE: These warnings apply to the XM-3300/XM-3320/XM-3340/XM-3360.

- ! **Safety Warnings**
 - Read all user documentation before powering this device. All Xirrus interconnected equipment should be contained indoors. This product is not suitable for outdoor operation. Please verify the integrity of the system ground prior to installing Xirrus equipment. Additionally, verify that the ambient operating temperature does not exceed 50°C.
- ! **Explosive Device Proximity Warning**
 - Do not operate the XM-3300/XM-3320/XM-3340/XM-3360 unit near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.
- ! **Lightning Activity Warning**
 - Do not work on the XM-3300/XM-3320/XM-3340/XM-3360 or connect or disconnect cables during periods of lightning activity.
- ! **Circuit Breaker Warning**
 - The XM-3300/XM-3320/XM-3340/XM-3360 relies on the building's installation for over current protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A (U.S.) or 240 VAC, 10A (International) is used on all current-carrying conductors.

Translated Safety Warnings

NOTE: These warnings apply to the XM-3300/XM-3320/XM-3340/XM-3360

Avertissements de Sécurité

- ! **Sécurité**
 - Lisez l'ensemble de la documentation utilisateur avant de mettre cet appareil sous tension. Tous les équipements Xirrus interconnectés doivent être installés en intérieur. Ce produit n'est pas conçu pour être utilisé en extérieur. Veuillez vérifier l'intégrité de la terre du système avant d'installer des équipements Xirrus. Vérifiez également que la température de fonctionnement ambiante n'excède pas 50°C.
- ! **Proximité d'appareils explosifs**
 - N'utilisez pas l'unité XM-3300/XM-3320/XM-3340/XM-3360 à proximité d'amorces non blindées ou dans un environnement explosif, à moins que l'appareil n'ait été spécifiquement modifié pour un tel usage.
- ! **Foudre**
 - N'utilisez pas l'unité XM-3300/XM-3320/XM-3340/XM-3360 et ne branchez pas ou ne débranchez pas de câbles en cas de foudre.
- ! **Disjoncteur**
 - L'unité XM-3300/XM-3320/XM-3340/XM-3360 dépend de l'installation du bâtiment pour ce qui est de la protection contre les surintensités. Assurez-vous qu'un fusible ou qu'un disjoncteur de 120 Vca, 15 A (États-Unis) ou de 240 Vca, 10 A (International) maximum est utilisé sur tous les conducteurs de courant.

Hardware Warranty Agreement

NOTE: This agreement applies to the XM-3300/XM-3320/XM-3340/XM-3360 Management Appliance.

PLEASE READ THIS CAREFULLY BEFORE USING THIS PRODUCT.

BY USING THIS PRODUCT, YOU ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTOOD ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT AND THAT YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, RETURN THE UNUSED PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.

LIMITED WARRANTY. Xirrus warrants that for a period of one year from the date of purchase by the original purchaser ("Customer"): (i) the Xirrus Equipment") will be free of defects in materials and workmanship under normal use; and (ii) the Equipment substantially conforms to its published specifications. Except for the foregoing, the Equipment is provided AS IS. This limited warranty extends only to Customer as the original purchaser. Customer's exclusive remedy and the entire liability of Xirrus and its suppliers under this limited warranty will be, at Xirrus' option, repair, replacement, or refund of the Equipment if reported (or, upon request, returned) to the party supplying the Equipment to Customer. In no event does Xirrus warrant that the Equipment is error free or that Customer will be able to operate the Equipment without problems or interruptions.

This warranty does not apply if the Equipment (a) has been altered, except by Xirrus, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Xirrus, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident, or (d) is used in ultra-hazardous activities.

DISCLAIMER. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW.

IN NO EVENT WILL XIRRUS OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE THE EQUIPMENT EVEN IF XIRRUS OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL XIRRUS' OR ITS SUPPLIERS' LIABILITY TO CUSTOMER, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, EXCEED THE PRICE PAID BY CUSTOMER. THE FOREGOING LIMITATIONS SHALL APPLY EVEN IF THE ABOVE-STATED WARRANTY FAILS OF ITS ESSENTIAL PURPOSE. SOME STATES DO NOT ALLOW LIMITATION OR EXCLUSION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES.

The above warranty DOES NOT apply to any evaluation Equipment made available for testing or demonstration purposes. All such Equipment is provided AS IS without any warranty whatsoever.

Customer agrees the Equipment and related documentation shall not be used in life support systems, human implantation, nuclear facilities or systems or any other application where failure could lead to a loss of life or catastrophic property damage, or cause or permit any third party to do any of the foregoing.

All information or feedback provided by Customer to Xirrus with respect to the Product shall be Xirrus' property and deemed confidential information of Xirrus.

Equipment including technical data, is subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Equipment.

This Agreement shall be governed by and construed in accordance with the laws of the State of California, United States of America, as if performed wholly within the state and without giving effect to the principles of conflict of law. If any portion hereof is found to be void or unenforceable, the remaining provisions of this Warranty shall remain in full force and effect. This Warranty constitutes the entire agreement between the parties with respect to the use of the Equipment.

Manufacturer is Xirrus, Inc. 2101 Corporate Center Drive Thousand Oaks, CA 91320.

Table of Contents

Bulleted items that do not appear in the main TOC list (they are part of the front matter, prior to this Table of Contents) include the following:

- Trademarks
- Notices
- Safety Warnings
- Translated Safety Warnings
- Hardware Warranty Agreement

List of Figures..... xiii

Introduction 1

 The Xirrus Family of Products 1

 About this User’s Guide 3

 Organization 3

 Notes and Cautions 5

 The User’s Guide as a PDF Document 5

 Hyperlinks 6

 XMS Product Overview 7

 Extended Management Capability 7

 A Scalable Solution 7

 Key Features and Benefits 9

 Centralized Management 9

 Scalability 9

 No Traffic Jams 9

 Security Management 9

 Powerful Graphical Interface 9

 Performance Monitoring 10

 Advanced Functionality 10

 Centralized Configuration Management 10

 Network Monitoring and Reporting 11

Xirrus Management System Products	13
XM-3300, XM-3320, XM-3340, XM-3360	13
About the XM-3320, XM-3340, and XM-3360	14
About the XM-3300	15
About XA-3300-CC	16
XA-3300-CC System Requirements	16
Installing the XA-3300-CC Application	17
 Getting Started with XMS.....	21
XMS Port Requirements	22
Starting and Managing the XMS Server	25
Initial Server Setup for Linux-based Management Appliances	28
Starting the XMS Client Interface	29
XMS Java Client—Minimum System Requirements	29
Java Client	30
Licensing the XMS Server	35
Discovering Networks and Arrays	37
Closing Down the Java Client Interface	37
Shutting Down the XMS Server	38
 The XMS Java Client Interface.....	39
Major Components of the Client Work Space	40
Menu Bar	41
Toolbar	42
Tree	43
Status Bar	44
Tool Tips	44
Other Navigation Tools	45
Main Viewing Area	46
Basic Window Operations	53
Navigating through Active Windows	53
Detaching a Window from the Client	53
Minimizing and Maximizing Windows	54
Arranging Windows	55

Closing a Window	56
Basic Table Operations	57
Page Navigation Buttons	59
Sorting Table Details	60
Searching for Table Entries	61
Rearranging and Resizing Columns in a Table	62
Viewing Row Details	62
Searching for Events	64
Keyboard Shortcuts	65
 Discovering the Network	67
Overview of Starting Discovery	68
How Discovery Works	70
Viewing Your Discovered Networks and Devices	72
Scheduling Discovery	74
Adding a Network	78
Adding or Deleting Array Shell Authentication Entries	80
Adding or Deleting SNMPv2 and SNMPv3 Entries	81
Modifying a Network	84
Excluding a Network from Discovery	84
Rediscovering a Network	85
Deleting a Network	86
Adding an Array or PoGE Injector	87
Refreshing a Device	88
Deleting a Device	89
What If My Device Is Not in the Discovered Devices List?	89
 Using the Dashboard.....	91
Dashboard Overview	92
About Dashboard Data	92
Status	94
Stations	96
Performance	98
Security	100

Alarms	102
Monitoring Your Network	105
At First Glance	105
Viewing Events and Alarms for a Specific Array	105
Alarms	107
Severity Levels	110
Taking Action on an Alarm	110
Events	111
Syslog Events	112
Configuring Syslog and NTP Servers	112
Syslog Severity Levels	113
Reviewing Syslog Events	114
Email Notifications for Events and Alarms	115
Security - Managing Intrusions	119
The Devices Window	119
About Classifying Detected Devices	120
Classifying Rogue Devices via XMS	121
Classifying Rogue Devices on Arrays	121
Populating the XMS Devices Window	122
Detected Devices	123
Detected Devices List	124
Classification Buttons	125
Creating Classification Rules	126
Detecting Arrays List	128
Working with Maps	129
About Maps	129
Getting Started with Maps	130
The Map Window	132
The Map List	133
The Arrays List	134
The RF Heat Contour Map	136

Map Toolbar	138
Information Bars	140
Migrating Maps from Earlier Releases	142
Preparing Background Images for New Maps	142
Adding a New Map	144
Saving a Map (Important!)	145
Setting the Map's Scale	146
Adding Arrays to Maps	147
Orienting Arrays	150
Entering Environment Settings	151
Locating Devices	152
Changing Contour Map Colors	156
Deleting a Map	157
Managing Arrays Within Maps	158
Map Settings Window	160
Map Settings	160
Information Bars	161
Managing Your Wi-Fi Arrays.....	163
Arrays	165
The Arrays Window	166
Connecting to an Array	172
Viewing Array Status	172
Configuring an Array	174
Create Policies from Array	178
Enabling or Disabling IAPs	180
Auto-Configuring Channels on Multiple Arrays	181
Deleting an Array	182
Removing an Array from a Map	182
Assigning an Array to a Group	183
Applying Policies to an Array	185
Updating Array Software	185
Viewing Events and Alerts	186
Viewing Reports	186

Refreshing an Array	187
Rebooting an Array	187
Locating an Array on a Map	187
Managing a PoGE Injector	187
Managing Array Licenses	189
About Licensing and Upgrades	189
The Array Licensing Window	190
Exporting Array Licenses	191
Importing Array Licenses	192
Editing Array Licenses	194
Managing Pending Array Licenses	196
IAPs	198
The IAPs Window	198
Connecting to an IAP's Array	200
Configuring the RF Settings of an IAP	200
Viewing Events and Alerts (IAPs)	202
Stations	203
The Stations Window	203
Connecting to an Associated Array	205
Viewing Events and Alerts (Stations)	206
SSIDs	207
The SSIDs Window	207
Connecting to an SSID's Array	208
Configuring the SSID Settings	208
Viewing Events and Alerts (SSIDs)	210
PoGE Injectors	211
Add the Injector to XMS	212
Associate the Injector with an Array	212
Manage the Injector with XMS	213
Managing Configuration with Policies.....	215
Working with Policies	216
An Easy Way to Work With Policies	216
Using Policy Windows	218

Adding a Policy	219
Selecting the Columns Shown in a Policy Window	220
Refreshing the List	221
Modifying an Existing Policy	221
Executing a Policy	221
Deleting an Existing Policy	222
Global Policy	223
Creating a New Global (Default) Policy	223
Saving Your Global Policy	224
System Information	225
Creating a New System Policy	225
Saving Your System Information Policy	227
Management Control	228
Creating a New Management Policy	228
Saving Your Management Control Policy	238
Network	239
Creating a New Network Policy	239
Saving Your Network Policy	246
Services	247
Creating a New Services Policy	247
Saving Your Services Policy	258
VLAN	259
Creating a New VLAN Policy	260
Saving Your VLAN Policy	264
DHCP Server	265
Saving Your DHCP Server Policy	269
Security	270
Creating A New Security Policy	270
Saving Your Security Policy	286
SSIDs	287
Creating a New SSID Policy	287
Saving Your SSID Policy	300
User Groups	301
Creating a New User Group Policy	301
Saving Your User Group Policy	308

IAPs	309
Saving Your IAP Policy	315
RF	316
Creating a New RF Policy	317
Saving Your RF Policy	341
WDS	342
Creating a WDS Policy	343
Saving Your WDS Policy	347
Filters	348
Creating a New Filter Policy	348
Saving Your Filter Policy	353
Software Update	354
Creating a New Software Update Policy	354
Saving Your Software Update Policy	357
Web Page Redirect (WPR)	358
Creating a New Web Page Redirect Policy	358
Saving Your Web Page Redirect Policy	361
Configuration File (Advanced)	362
Creating a New Config File Policy	362
Saving Your Config File Policy	365
Groups	366
Creating A New Group	366
Applying Your Array Groups Policy	369
Audit	370
Managing Reports	371
About Reports	371
My Reports	373
Viewing a Report	375
New Report	378
Selection Criteria	384
Customize	387
Traffic Reports	388
Wireless Traffic	389

Wireless Errors	392
Station Traffic	394
Station Errors	397
Ethernet Traffic	399
Ethernet Errors	402
Station Reports	404
Associated Stations	405
Stations By Array	406
Unique Station Count	409
Array Reports	412
Array Inventory	412
Array Availability	414
RF Reports	416
Channel Usage	416
Security Reports	419
Rogue List	420
The XMS Web Client.....	423
Starting the Web Client	423
Web Client Modes	424
About Monitor Pages	424
About Configure Pages	425
About Reports Pages	427
About Settings Pages	428
Dashboard	431
Dashboard Overview	432
About Dashboard Data	432
Array and Radio Status	433
Recent Alarms	435
Stations	436
Rogue Overview	439
Arrays	441
About Using the Arrays Page	441
The Arrays List	444

The Arrays Toolbar	445
Radios	447
About Using the Radios Page	447
The Radios List	448
Stations	449
About Using the Stations Page	449
The Stations List	449
Rogues	451
About Using the Rogues Page	451
The Rogues List	452
Alarms	453
About Using the Alarms Page	453
The Alarms List	453
Events	455
About Using the Events Page	455
The Events List	456
Configure—Home Page	458
Network Settings	458
About Using the Network Settings Page	459
To Modify Rows Individually	459
To Modify Multiple Rows	460
To Export Network Settings	461
To Import Network Settings	464
Radio Settings	466
To Modify Rows Individually	467
To Modify Multiple Rows	468
To Export Radio Settings	469
To Import Radio Settings	469
Advanced Config	470
About Advanced Config Files	470
Advanced Config Page	471
Load from Array	473
Deploy Configuration	474
PoGE	476
Add Devices	477

Overview of Adding Devices	478
Add Devices	480
SNMPv2 And SNMPv3 Settings	482
SSH Users	485
Add Networks	486
Trap Receivers	488
Array Licenses	489
Custom Fields	489
Custom Fields Page	490
Custom Field Values	491
Custom Actions	493
XMS Administration	495
Country of Operation	496
User Accounts	497
Creating a New User Account	498
Saving Your XMS User Account	498
Backup Manager	499
Broadcast Message	500
About Managing the XMS Server	501
About the XMS Database	501
Managing XMS on Linux-based Management Appliances	502
Accessing the Web Client	503
Initial Server Setup	504
Web Client — Viewing XMS Server Status	506
Web Client — Network Settings	508
Web Client — Date and Time Settings	509
Web Client — Database Backup Settings	511
Web Client—Email Settings	515
Web Client — Polling Settings	516
Web Client — Changing the SSH Server Address	517
Web Client — Viewing Server Log Files	518
Web Client—Managing the XMS Server License	520
Web Client — Performing Upgrades	521

Web Client — Resetting the XMS Server	522
Managing XMS on Windows-based Systems	523
Starting the XMS Server on Windows-based Systems	524
Xirrus Server Management Tool (for Windows-based Servers)	526
XSMT - XMS Server Manager Tool	527
XSMT - Starting the XMS Server	529
XSMT - Shutting Down the XMS Server	531
XSMT - Database Tools	532
Re-initialize Database	532
Repair Database	533
XSMT - Software Manager	534
About the Installed Patch List	535
To Install a New Version of the XMS Server	535
XSMT - Advanced Settings	537
Changing Polling Frequency	537
Changing the SSH Server Address	539
Managing XMS Server Settings via the Web Client	540
Technical Support.....	541
General Hints and Tips for Xirrus Management Appliances	541
Frequently Asked Questions	542
Contact Information	544
Glossary of Terms.....	545
Index.....	553

List of Figures

Figure 1.	The Xirrus Management System	2
Figure 2.	Sample Network Topology	8
Figure 3.	XMS Java Client Dashboard.....	10
Figure 4.	Management Appliance (XM-3340, Ready for Rack-mount)	14
Figure 5.	Server Management Using the Web Client	15
Figure 6.	Server Status on XSMT	16
Figure 7.	Installation Wizard and End User License Agreement	17
Figure 8.	Choose an Install Location for the Application.....	18
Figure 9.	Unblocking Java	18
Figure 10.	Setting Up the Ports	19
Figure 11.	Reviewing Your Installation Parameters	19
Figure 12.	Installation Completes	20
Figure 13.	Sample Port Requirements for XMS	22
Figure 14.	Server Management using the Web Client	25
Figure 15.	XSMT Window, Showing Typical Running Status	27
Figure 16.	XMS Start Window	31
Figure 17.	Web Start Client Security Warning.....	32
Figure 18.	Client Login Window (Browser)	32
Figure 19.	Loading the XMS Client	33
Figure 20.	The Dashboard - XMS Java Client Window	33
Figure 21.	XMS Web Start Client Icon on desktop	34
Figure 22.	Client Login Window (Browser)	34
Figure 23.	XMS Server License	35
Figure 24.	Closing Down the Java Client Interface	37
Figure 25.	XMS Java Client Work Space	40
Figure 26.	Java Client Menu Bar	41
Figure 27.	Toolbar (Default Map View)	42
Figure 28.	Tree (Expanded).....	43
Figure 29.	Status Message	44
Figure 30.	Tool Tips	44
Figure 31.	Right-Click Menus (Arrays Window)	45

Figure 32.	Main Viewing Area	46
Figure 33.	Monitoring Window (Events).....	47
Figure 34.	Location (Map) Window	48
Figure 35.	Resources Window (Arrays).....	49
Figure 36.	Security Window	50
Figure 37.	Configuration Window (Security Policy).....	51
Figure 38.	Backup Manager.....	52
Figure 39.	Minimized Windows	54
Figure 40.	Horizontal Tiling of Windows.....	55
Figure 41.	Typical Table (Events).....	57
Figure 42.	Show All Events After a Search.....	58
Figure 43.	Table Sorting Arrows	60
Figure 44.	Searching for an Entry	61
Figure 45.	Row Details (Expanded from a Row)	63
Figure 46.	Using the Search Engine	64
Figure 47.	Managing Discovery of Devices.....	69
Figure 48.	Discover Devices Window	72
Figure 49.	Network Discovery Schedule	74
Figure 50.	Viewing the Discovery Schedule.....	75
Figure 51.	Scheduling the Discovery Process (Hourly)	76
Figure 52.	Scheduling the Discovery Process (Daily)	76
Figure 53.	Scheduling the Discovery Process (Monthly).....	77
Figure 54.	Adding a Network	78
Figure 55.	Network Added.....	78
Figure 56.	Network Discovery in Progress.....	79
Figure 57.	Network Discovery Finished	79
Figure 58.	Array Shell Authentication	80
Figure 59.	Adding an Array Shell Login.....	80
Figure 60.	SNMP v2 and SNMP v3 Configuration	81
Figure 61.	Adding an SNMPv3 Username	82
Figure 62.	Adding an SNMPv2 Community Name.....	83
Figure 63.	Modifying an Existing Network.....	84
Figure 64.	Disabling Discovery on a Network.....	84
Figure 65.	Deleting a Network	86
Figure 66.	Adding a Device	87

Figure 67.	Refreshing a Device	88
Figure 68.	Dashboard.....	91
Figure 69.	Dashboard - Status	94
Figure 70.	Dashboard - Stations	96
Figure 71.	Dashboard - Throughput.....	98
Figure 72.	Dashboard - Security.....	100
Figure 73.	Dashboard - Alarms	102
Figure 74.	Events and Alarms (By Array)	106
Figure 75.	Alarms Window.....	107
Figure 76.	Alarm Status Summary/Select Buttons	108
Figure 77.	Alarm List	109
Figure 78.	Reviewing Network Event Details.....	111
Figure 79.	Configuring a Syslog Server	113
Figure 80.	Syslog Window	114
Figure 81.	Filtering Syslog Entries	114
Figure 82.	Event Notifications List	116
Figure 83.	Event Notification Creation	117
Figure 84.	Security—Devices	119
Figure 85.	Devices Window—Detected Devices.....	123
Figure 86.	Editing Classification Rules	126
Figure 87.	Devices Window—Detecting Arrays	128
Figure 88.	Main Map with RF Heat Contours Enabled	132
Figure 89.	The Map List.....	133
Figure 90.	The Arrays List.....	134
Figure 91.	Finding an Entry in the Arrays List	134
Figure 92.	Main Map Showing RF Heat Contours	136
Figure 93.	The Map Toolbar	138
Figure 94.	The Map Data Information Bar	141
Figure 95.	The Array Data Information Bar	141
Figure 96.	Maps List.....	144
Figure 97.	Map Settings Window	144
Figure 98.	Calibrating the Map Scale	146
Figure 99.	Edit Map Scale (Calibrate Distance)	147
Figure 100.	Adding an Array to a Map.....	148
Figure 101.	Resizing and Moving Arrays	149

Figure 102. Rotating an Array	150
Figure 103. Entering Environment (Wall) Settings	151
Figure 104. Using the Location Feature	152
Figure 105. Determining Position	153
Figure 106. Changing Contour Map Colors	156
Figure 107. Displaying Arrays Within Maps	158
Figure 108. Array Management Drop-down Menu	159
Figure 109. Map Settings Page	160
Figure 110. Map Settings - Information Bars.....	161
Figure 111. Table Column Chooser	163
Figure 112. Arrays Window	166
Figure 113. Array Status Summary/Select Buttons	167
Figure 114. All Array Throughput.....	168
Figure 115. Array List.....	169
Figure 116. Menu Items for Configuring Arrays.....	170
Figure 117. Array Login Window	172
Figure 118. Array Status Summary	173
Figure 119. Configuring an Array	174
Figure 120. Configuring an Array	175
Figure 121. Task Results (success)	176
Figure 122. Save Results	176
Figure 123. Task Results (Failure).....	176
Figure 124. Create Policies from Array	178
Figure 125. Confirm Policies to be Created (First and Subsequent times)	179
Figure 126. Results of Create Policies from Array	180
Figure 127. Auto Configure Confirmation Dialog	181
Figure 128. Deleting an Array	182
Figure 129. Assigning a Group.....	183
Figure 130. Assigning Policies.....	185
Figure 131. Updating Array Software Image	186
Figure 132. Viewing Events and Alerts.....	186
Figure 133. Rebooting an Array	187
Figure 134. Array License Management - Deployed Licenses	190
Figure 135. Exporting Array Licenses	191
Figure 136. Sample Export File.....	192

Figure 137. Importing Array Licenses.....	193
Figure 138. Select Array Licenses to Edit.....	194
Figure 139. Editing Array Licenses.....	195
Figure 140. Array Licenses Pending Deployment.....	196
Figure 141. IAPs Window	198
Figure 142. RF Settings	201
Figure 143. Viewing Events and Alerts.....	202
Figure 144. Stations Window.....	203
Figure 145. Viewing Events and Alerts.....	206
Figure 146. SSIDs Window	207
Figure 147. SSID Settings	209
Figure 148. Viewing Events and Alerts.....	210
Figure 149. Injector and Array Associations	212
Figure 150. Associating Injector and Array Ports.....	213
Figure 151. Policy Window - Executing a Policy.....	218
Figure 152. Adding a Policy	219
Figure 153. Selecting the Attributes of a Policy Window.....	220
Figure 154. Modifying and Deleting a Policy	222
Figure 155. List of Global Policies.....	223
Figure 156. Global (Default) Policy Settings	224
Figure 157. List of System Policies.....	225
Figure 158. System Settings	226
Figure 159. List of Management Policies	228
Figure 160. Management Settings.....	229
Figure 161. SNMP Settings	232
Figure 162. SNMPv3 Settings	234
Figure 163. Admin Settings	236
Figure 164. Adding an Administrator Account to the Admin List.....	236
Figure 165. Console Settings.....	237
Figure 166. List of Network Policies.....	239
Figure 167. Network Interface Ports.....	240
Figure 168. Network Settings (10/100 Fast Ethernet).....	241
Figure 169. Network Settings (Gigabit 1)	244
Figure 170. List of Services Policies	247
Figure 171. DNS Server Settings	248

Figure 172. NTP Settings.....	250
Figure 173. NetFlow Settings.....	252
Figure 174. System Log Server Settings	253
Figure 175. Standby Mode Settings	256
Figure 176. Wi-Fi Tag Settings	257
Figure 177. VLAN Policy List.....	259
Figure 178. VLAN Settings	260
Figure 179. VLAN List Settings.....	261
Figure 180. List of DHCP Server Policies	265
Figure 181. DHCP Server Settings	266
Figure 182. DHCP List Settings.....	267
Figure 183. List of Security Policies	270
Figure 184. Security Settings.....	272
Figure 185. RADIUS Management	276
Figure 186. Adding Internal RADIUS Users.....	280
Figure 187. MAC Access List.....	282
Figure 188. Adding a MAC Address to the MAC Access List	283
Figure 189. MAC Access List.....	283
Figure 190. Admin RADIUS Management.....	284
Figure 191. List of SSID Policies.....	287
Figure 192. SSID Settings	288
Figure 193. SSID List Entry	289
Figure 194. SSID Security Settings	297
Figure 195. SSID Settings	299
Figure 196. Customizing an Internal Login or Splash Page.....	300
Figure 197. List of User Group Policies.....	301
Figure 198. User Group Settings	302
Figure 199. Adding an entry to the User Group List	304
Figure 200. Arrangement of IAPs (XN16 Array)	309
Figure 201. List of IAP Policies.....	309
Figure 202. IAP Settings (Policy Details)	310
Figure 203. IAP Settings (For Selected IAP)	311
Figure 204. List of RF Policies.....	316
Figure 205. Radiated Coverage Patterns.....	316
Figure 206. LED Locations (XN16)	318

Figure 207. Global RF Settings	319
Figure 208. Fast Roaming Settings.....	328
Figure 209. 802.11a RF Settings	331
Figure 210. 802.11/g RF Settings	333
Figure 211. 802.11n RF Settings.....	337
Figure 212. LED Settings	340
Figure 213. Configuring a WDS Link.....	342
Figure 214. WDS Policy Window	342
Figure 215. WDS Client Links	344
Figure 216. WDS Client Link Settings.....	344
Figure 217. WDS Client IAP Window	346
Figure 218. WDS - Assign IAP to Client	347
Figure 219. List of Filter Policies	348
Figure 220. Filter Policy Details	349
Figure 221. Filter List Details.....	351
Figure 222. Filters Setting Details	352
Figure 223. List of Software Policies.....	354
Figure 224. Software Update	355
Figure 225. File Chooser	356
Figure 226. List of WPR Policies	358
Figure 227. Web Page Redirect.....	359
Figure 228. WPR File Upload to XMS Server	360
Figure 229. Selecting WPR File List Entries.....	361
Figure 230. List of Config File Policies	362
Figure 231. Create Config File Policy	363
Figure 232. Configuration File Edit and View Window.....	364
Figure 233. List of Groups.....	366
Figure 234. Array Group	367
Figure 235. Policy Details.....	368
Figure 236. Viewing the Audit Details.....	370
Figure 237. My Reports Window	373
Figure 238. Actions for Reports.....	374
Figure 239. Archived Reports List	375
Figure 240. Viewing a Report	375
Figure 241. Report Including Charts	376

Figure 242. Emailing a Report.....	377
Figure 243. List of New Report Types.....	378
Figure 244. Create New Report Page	379
Figure 245. Report Queue	383
Figure 246. Customize Report Header Page	387
Figure 247. Wireless Traffic Report	390
Figure 248. Wireless Errors Report.....	393
Figure 249. Station Traffic Report (Tx+Rx)	395
Figure 250. Station Errors Report.....	398
Figure 251. Ethernet Traffic Report	400
Figure 252. Ethernet Errors Report.....	403
Figure 253. Station Association	406
Figure 254. Station Association (By Array) Report	408
Figure 255. Unique Station Count Report	410
Figure 256. Array Inventory Report.....	413
Figure 257. Array Availability Report.....	414
Figure 258. Channel Usage Report	417
Figure 259. Rogue List Report.....	421
Figure 260. XMS Start Window	423
Figure 261. Mode Selection in XMS Web Client	424
Figure 262. XMS Web Client Monitor Functions.....	425
Figure 263. XMS Web Client Configure Functions	426
Figure 264. XMS Web Client Reports Functions.....	427
Figure 265. XMS Web Client Settings Functions	428
Figure 266. Settings Menus for Windows and Linux Servers	429
Figure 267. Dashboard.....	431
Figure 268. Dashboard - Array and Radio Status.....	433
Figure 269. Dashboard - Recent Alarms	435
Figure 270. Dashboard - Station Count.....	436
Figure 271. Dashboard - Top Station Manufacturers.....	437
Figure 272. Dashboard - Station Connection Metrics	438
Figure 273. Dashboard - Rogue Overview	439
Figure 274. Arrays Page	441
Figure 275. Table Column Chooser	442
Figure 276. The Array Page Toolbar.....	445

Figure 277. Pull Diagnostic Logs	445
Figure 278. Radios Page	447
Figure 279. Stations Page	449
Figure 280. Rogues Page	451
Figure 281. Alarms Page	453
Figure 282. Events Page.....	455
Figure 283. Network Settings Page.....	458
Figure 284. Editing the Network Settings Page.....	460
Figure 285. Bulk Configuration (Network Settings)	461
Figure 286. Export Network Settings	463
Figure 287. Exported Network Settings File	463
Figure 288. Import Network Settings.....	464
Figure 289. Verify Imported Network Setting Values	465
Figure 290. Radio Settings Page	466
Figure 291. Editing the Radio Settings Page	467
Figure 292. Bulk Configuration (Radio Settings).....	468
Figure 293. Advanced Config Page	471
Figure 294. Advanced Config Editor.....	472
Figure 295. Load from Array.....	473
Figure 296. Select Advanced Config File to Deploy.....	474
Figure 297. Select Arrays for Deployment.....	475
Figure 298. Select Deployment Options.....	475
Figure 299. Select Deployment Options.....	476
Figure 300. Managing Discovery of Devices.....	479
Figure 301. Discover a Single Device	480
Figure 302. Discover a Range of IP Addresses	481
Figure 303. Discover a List of IP Addresses	481
Figure 304. Review Results of Adding Devices.....	482
Figure 305. SNMPv3 Users	483
Figure 306. SNMPv2 Settings	484
Figure 307. Adding SSH Users.....	485
Figure 308. Add Networks for Discovery.....	486
Figure 309. Trap Receivers.....	488
Figure 310. Custom Fields Page.....	490
Figure 311. Custom Field Values—Adding a single value	491

Figure 312. Bulk Configuration (Custom Field Values)	492
Figure 313. Custom Actions Page	493
Figure 314. Country of Operation.....	496
Figure 315. List of XMS User Accounts.....	497
Figure 316. Select Policy Attributes (XMS User Accounts).....	497
Figure 317. Manage User Accounts	498
Figure 318. Database Backup Manager.....	499
Figure 319. Broadcast Message	500
Figure 320. Server Management using the Web Client	502
Figure 321. Starting the Web Client.....	503
Figure 322. Changing Network Settings.....	504
Figure 323. The Status Page	506
Figure 324. Changing Network Settings.....	508
Figure 325. Changing Date and Time Settings	509
Figure 326. Changing Database Backup Settings	511
Figure 327. Scheduling Backups	512
Figure 328. Restoring Backups	513
Figure 329. Changing the Email Server	515
Figure 330. Changing Polling Rate	516
Figure 331. Changing the SSH Server	517
Figure 332. Viewing Log Files	518
Figure 333. Viewing a Selected Log File	519
Figure 334. Multiple Log Files.....	519
Figure 335. XMS Server License	520
Figure 336. Upgrading XMS Software	521
Figure 337. Resetting XMS	522
Figure 338. Xirrus Server Management Tool - XMS Server Manager	523
Figure 339. Start XMS as a Windows Service.....	524
Figure 340. Xirrus Server Management Tool - XMS Server Manager	526
Figure 341. Status of Services, Showing Normal Status	527
Figure 342. Status of Offline Activities.....	528
Figure 343. Server Startup Progress	530
Figure 344. Server is Up (XSMT).....	530
Figure 345. Server Shutdown Progress	531
Figure 346. Status for Stopped XMS Server.....	532

Figure 347. XSMT Software Manager 534

Figure 348. Select a Patch File..... 535

Figure 349. XSMT Advanced Menu Options 537

Figure 350. Changing Polling Frequency 538

Figure 351. Changing the SSH Server 539

Figure 352. Changing Advanced Settings from a Browser 540

Introduction

This section introduces the Xirrus Management System (XMS) and the Xirrus Management Appliance, including an overview of key features and benefits. It also includes an outline of how this User's Guide is organized. Section headings for this chapter include:

- **"The Xirrus Family of Products" on page 1**
- **"About this User's Guide" on page 3**
- **"XMS Product Overview" on page 7**
- **"Key Features and Benefits" on page 9**

The Xirrus Family of Products

The Xirrus family of products includes the following items:

- **Xirrus Management System (XMS)**
XMS is a powerful management tool, designed to manage your Wi-Fi Arrays and managed Power over Gigabit Ethernet injectors from anywhere in the network — ideal for large scale Wi-Fi deployments. XMS supports all Array models including the XN series that offers IEEE 802.11n protocol support. The XMS server is available pre-installed on the Xirrus Management Appliance, or you may install it on your own hardware:
 - **Xirrus Management Appliance**
The Management Appliance is a dedicated network device tailored to run XMS, and designed to manage up to 1000 Wi-Fi Arrays. XMS is furnished pre-installed. There are two families of Appliances — the Linux-based XM-3320, XM-3340, and XM-3360; and the Microsoft Windows-based XM-3300.
 - **Xirrus Application — XMS Server Software (Xirrus Part Number XA-3300-CC)**
The XA-3300-CC application package allows you to install and run the XMS server software on your own server device.

- **Xirrus Wi-Fi Array**

The Xirrus Wi-Fi Array is specifically designed for the Enterprise market, utilizing up to 16 Integrated Access Points (IAPs). Multiple versions of the Array with different numbers of Integrated Access Points (IAPs) support a variety of deployment applications: 16 IAPs (XN16, XS16, XS-3900), 12 IAPs (XN12), 8 IAPs (XN8, XS8, XS-3700), and 4 IAPs (XN4, XS4, XS-3500). For more information, refer to the *Xirrus Wi-Fi Array User's Guide*, part number 800-0006-001.

- **Xirrus XP Power System**

Xirrus power options include the XP1, XP2, and XP8 Power over Gigabit Ethernet (PoGE) modules, eliminating the need to run separate power cabling. All of these are available in managed versions, allowing your power supplies to be managed by XMS as part of your Wi-Fi network.

Figure 1 illustrates the elements of the Xirrus Management System. The XMS server may run on hardware supplied by Xirrus or by you. Users start the XMS client simply by entering the URL of the XMS server on a web browser on their computers. The XMS server manages a number of Wi-Fi Arrays via SNMP.

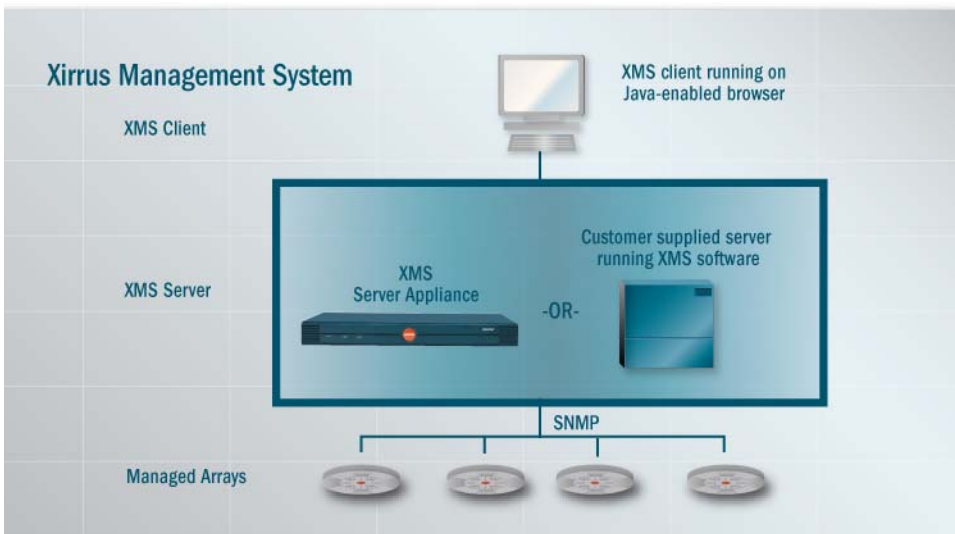


Figure 1. The Xirrus Management System

About this User's Guide

Detailed information and procedures have been provided in this User's Guide that will enable network administrators to run XMS on the Xirrus Management Appliance or to install and run XMS on their own hardware, to understand and navigate the XMS client interface, and to successfully manage their network of Wi-Fi Arrays from a central location. XMS may be installed on your own Windows Server-based platform, or comes pre-installed on the Management Appliance which was specifically designed by Xirrus to host XMS. This Guide does not cover the installation or management of Arrays in isolation from XMS. For procedures that deal with Arrays not centrally managed by XMS, refer to the *Xirrus Wi-Fi Array User's Guide*, part number 800-0006-001.

Organization

This User's Guide is organized by function under the following headings:

- **Introduction**
Provides an overview of the product, including its key features and benefits.
- **Xirrus Management System Products**
This chapter provides an overview of what you can expect when you install your Xirrus management product for the first time—information you need to know if you want to make informed decisions when using the system. It also provides instructions to help you complete a successful installation.
- **Getting Started with XMS**
Discusses starting, stopping, and managing the XMS server and client software. Provides procedures for initial setup of XMS, such as setting a network address and discovering the Wi-Fi network.
- **The XMS Java Client Interface**
Presents examples of the product's Java-based client interface, including the content and structure of its major components, and includes detailed descriptions of navigation and management tools.

- **Discovering the Network**
Provides instructions for discovering networks and Wi-Fi Arrays, and adding them to XMS.
- **Using the Dashboard**
Describes the features and use of the Dashboard in the Java client, an at-a-glance overview of network security and performance.
- **Monitoring Your Network**
Discusses the tools provided in the Java client that allow you to monitor and manage any system events and alarms flagged by the system, including syslog events, network events, alarms, and auditing.
- **Security - Managing Intrusions**
Discusses management of the security status of the network using the Java client, including known and rogue APs and types of encryption in use.
- **Working with Maps**
Introduces you to the location/RF contour map in the Java client, and provides instructions for managing your maps and map layouts. It also shows you how to prepare map background images.
- **Managing Your Wi-Fi Arrays**
Provides instructions for managing discovered Arrays with the Java client, and includes configuring wireless stations, individual IAPs, and SSIDs. It also shows you how to view and assign properties to your Arrays.
- **Managing Configuration with Policies**
Shows you how to use the Java client to create and manage the configuration policies that are used by your Arrays (and groups of Arrays) to establish a uniform and effective method for administering security, users and groups, and other wireless network management criteria.
- **Managing Reports**
XMS generates detailed performance and status reports about the network, all Arrays within the network, individual IAPs contained

within each Array, and client stations. This chapter provides instructions for reviewing and managing these reports in the web client.

- **The XMS Web Client**

Describes how to use the web client interface (a fast alternative to the Java client), including the Wi-Fi network monitoring and configuration tools, and XMS server management tools.

- **XMS Administration**

Provides instructions for managing the XMS database and other administrative tasks, including how to review the current status of the database, how to schedule and create backups, and how to restore the database from the server.

- **Technical Support**

Offers guidance to resolve technical issues, some general hints and tips to enhance your product experience, and Xirrus contact information.

- **Glossary of Terms**

Provides an explanation of terms directly related to XMS product technology, organized alphabetically.

Notes and Cautions

The following symbol is used throughout this User's Guide:

- ! *This symbol is used for cautions. Cautions provide critical information that may adversely affect the performance of the product.*

NOTE: General notes provide useful supplemental information.

The User's Guide as a PDF Document

The User's Guide is available as a secure PDF (Portable Document Format) file and can be viewed using the Adobe® Acrobat Reader® product. It cannot be edited or modified. If you don't have Acrobat Reader, you can download it free-of-charge from: <http://www.adobe.com>.

Hyperlinks

If you click on body text that appears in the color **TEAL** (with the exception of headings or notes) the embedded hyperlink within the text will immediately take you to the referenced destination. All cross-references, including the **Table of Contents**, page numbers within the **List of Figures** and the **Index**, and embedded text have associated hyperlinks. If you want to return to the reference source, you can do this by clicking on Acrobat's **previous page** button.

XMS Product Overview

The Xirrus Management System extends the capabilities of the Wi-Fi Array's Web Management Interface (WMI) and Command Line Interface (CLI) to multiple Wi-Fi Arrays over an entire network. XMS includes the same configuration, performance monitoring, security, fault management, and reporting mechanisms used in the Wi-Fi Array, but adds an aggregate view of an entire network of Arrays across Layer 2 and Layer 3 boundaries.

Extended Management Capability

Providing an at-a-glance overview of network conditions and throughput, XMS reports all threats to the network—with full event logs for rogue access points, network health and Wi-Fi Array performance

With its powerful discovery feature and map-based organization of your Wi-Fi Arrays, XMS streamlines the management of Array configurations.

XMS allows IT administrators to manage configurations, establish policies, schedule firmware upgrades across multiple Wi-Fi Arrays, and create groups of Wi-Fi Arrays to simplify repetitive tasks. Policies may be created automatically by copying the existing configuration of selected Arrays. XMS also offers different administrative levels that allow Help Desk staff to monitor their network and its client activity, and restrict network setting changes to specific staff members. All of these features allow the IT department to actively monitor and manage the health of their wireless network from anywhere using a browser.

A Scalable Solution

The Xirrus centralized management technology is available as a dedicated Management Appliance or as a software-only solution (XA-3300-CC) that can be installed on an existing server in the IT closet. For larger networks, licenses are available to add support for additional Wi-Fi Arrays.

Together with its family of Wi-Fi Arrays, Xirrus created XMS to facilitate faster and more cost-effective high capacity Wi-Fi rollouts across large campus environments and branch office locations. This total solution delivers Gigabit-class wireless access with maximum deployment flexibility across a wide range of

locations, from a single site corporate headquarters environment to large multi-site branch offices.

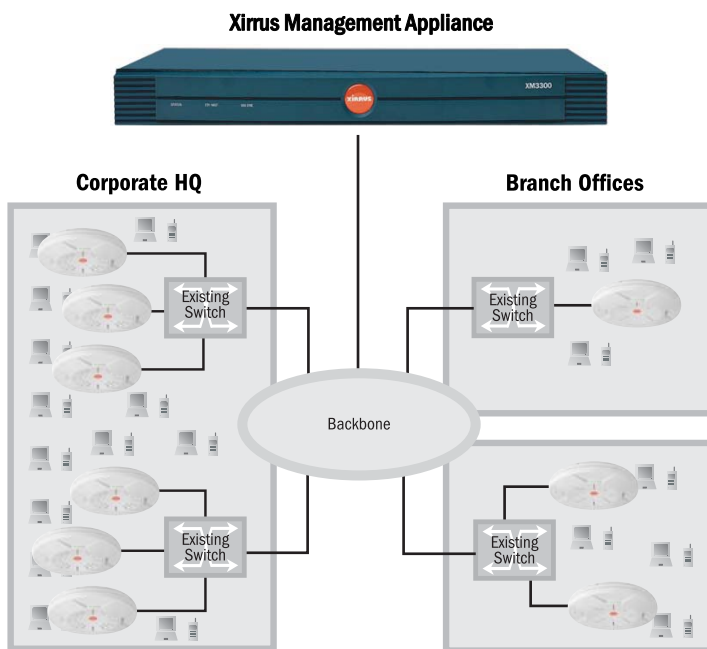


Figure 2. Sample Network Topology

XMS monitors wireless performance and gathers detailed reporting and statistical data for each Wi-Fi Array residing in the network, or for the entire network as a whole. It also allows you to schedule firmware updates for individual Wi-Fi Arrays or groups of Arrays to ensure that your Array firmware is up-to-date and consistent across the network.

Key Features and Benefits

This section describes some of the key product features and the benefits you can expect when deploying the XMS to configure and manage your network of Wi-Fi Arrays.

Centralized Management

Allows you to view and manage your entire wireless network at Layer 3 using your existing Ethernet infrastructure. In addition, XMS discovers, authenticates and configures new Wi-Fi Arrays to the network making large scale deployments quick and easy. Policies ensure consistent configuration of Arrays across the network, and they are easily created by copying the configuration of a “known-good” Array.

Scalability

With its ability to support over 500 Wi-Fi Arrays per XMS server, XMS allows your network to grow as your business grows.

No Traffic Jams

Because the XMS resides outside the data path, performance bottlenecks and points of failure are eliminated.

Security Management

Defines and distributes security policies for the entire network, and allows you to set encryption, authentication, access times, and guest user access policies for secure Wi-Fi Array rollouts.

Powerful Graphical Interface

XMS's client interfaces provide all the tools and features that are necessary to ensure your network is configured and managed effectively and securely. The interfaces are easy to use and can be accessed from any location using a Web browser.

The XMS Dashboard (**Figure 3**) provides an at-a-glance overview of the security and performance of your network.

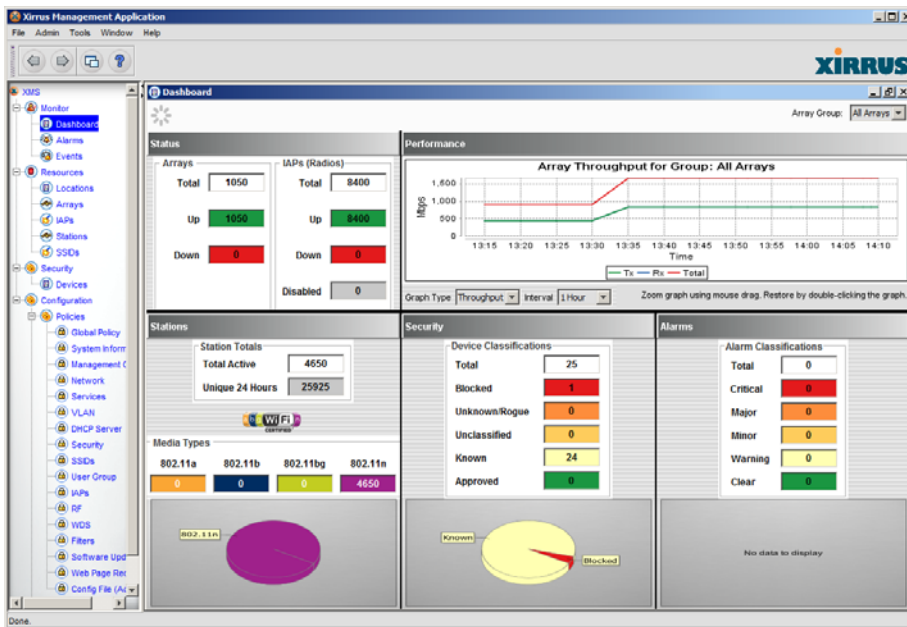


Figure 3. XMS Java Client Dashboard

Performance Monitoring

Continually monitors wireless performance and will alert you to interference or other issues before network problems have an opportunity to escalate.

Advanced Functionality

XMS provides a convenient platform to add feature enhancements, such as location-based tracking, by taking advantage of the Wi-Fi Array's superior "directionally-aware" capabilities.

Centralized Configuration Management

Allows you to schedule firmware updates for individual Wi-Fi Arrays or groups of Arrays at specific times. In addition, XMS can archive any previous version(s) of firmware that your network has used.

Network Monitoring and Reporting

XMS manages all alerts and alarms to determine how to respond to potential faults in the network. The unit also monitors your network's wireless performance and provides detailed reporting and statistical data for each Wi-Fi Array, group of Arrays, or individual IAPs (Integrated Access Points).

Xirrus Management System Products

The Xirrus Management system is offered in two forms:

- **XM-3300, XM-3320, XM-3340, XM-3360**—dedicated servers that are furnished with XMS software pre-installed and ready to go.
- **About XA-3300-CC**—a software-only version of XMS that you may install on your own server hardware.

XM-3300, XM-3320, XM-3340, XM-3360

The Xirrus XM-3300, XM-3320, XM-3340, and XM-3360 Management Appliances operate as dedicated servers for the Xirrus Management System (XMS). The Management Appliance can manage up to 1000 Wi-Fi Arrays over a Layer 3 network, ideal for campus, multi-site enterprise, or other large scale Wi-Fi deployments. The Management Appliance is provided as a 1U or 2U rack-mountable chassis offering a centralized mechanism for managing Array configuration, security settings, and software revisions while monitoring your Wi-Fi network's performance and health. You can also control managed versions of Xirrus Power over Gigabit Ethernet (PoGE) power injectors and use them to turn Arrays on and off.

All models are delivered with XMS pre-installed and ready to start up automatically when the system is booted.

The Management Appliance has the following advantages:

Compact

1U or 2U high rack-mountable (or free standing) unit facilitates easy installation, and offers high performance connections to your network's backbone and isolation of all management traffic.

Enterprise Class

As a dedicated network appliance, it ensures maximum uptime and reliability, and features dual 1 Gbps uplink ports for reliability, seamless integration, and installation anywhere in your network.

No Traffic Jams

Unlike management solutions that generally reside in the network's data path, the Management Appliance does not interfere with the network's data traffic.

About the XM-3320, XM-3340, and XM-3360



Figure 4. Management Appliance (XM-3340, Ready for Rack-mount)

The latest Xirrus Management Appliance models are based on the Linux operating system. The XM-3360 offers the highest capacity, managing networks of 1000 Arrays.

The Management Appliance operates as a network-based device. You communicate with it via the network using a web browser or via Telnet/SSH, rather than connecting a monitor and keyboard to it directly.

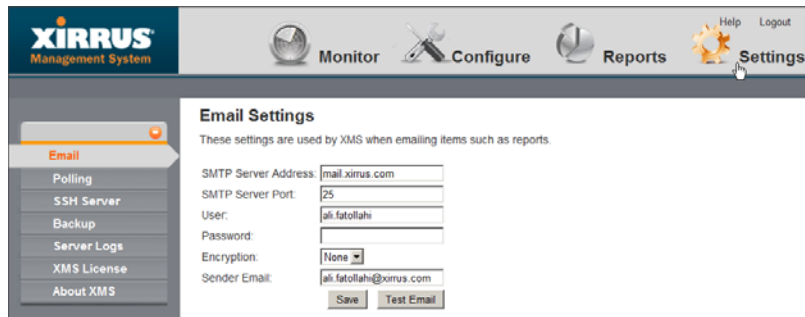


Figure 5. Server Management Using the Web Client

Installation and requirements are described in the *XM-3320/ XM-3340/ XM-3360 Management Appliance Quick Installation Guide*, PN 812-0073-001. The XMS server is managed using the browser-based XMS web client (**Figure 5**). For more information on using the web client, see **“Managing XMS on Linux-based Management Appliances” on page 502**.

About the XM-3300

The XM-3300 is a legacy model, based on the Microsoft Windows operating system.

Installation and requirements are described in the *XM-3300 Management Platform Quick Installation Guide*, PN 812-0016-001. The XMS server on this model is managed using the Xirus Server Management Tool (XSMT—see **Figure 6**). For more information on using XSMT, see **“Managing XMS on Windows-based Systems” on page 523**.

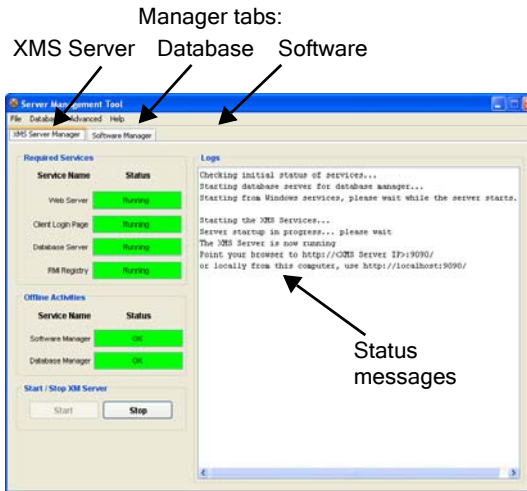


Figure 6. Server Status on XSMT

While the XM-3300 is a network-based device that will normally be used via the network, a monitor and keyboard/mouse should be connected to it. The factory default Windows login for the XM-3300 is **Administrator/Xirrus!23** (note the exclamation mark).

About XA-3300-CC

XA-3300-CC is a software only version of the XMS server that you install on your own hardware running a Windows-based operating system. The following sections describe its requirements and how to install it.

XA-3300-CC System Requirements

The recommended requirements for the system hosting the XMS server are based on the scale of the Wi-Fi Array network to be managed—small, medium, or large.

Please see www.xirrus.com for specifications and system requirements for the scale of the network to be managed.

Installing the XA-3300-CC Application

1. If XMS is not currently installed on your server, proceed to **Step 2**.

If you already have a version of XMS installed on your computer, please check the Release Notes to see if there are any special upgrade directions.

If there are no special instructions, you should use the **Install Patch** feature of the XSMT-Software Manager to install the software update. See **“To Install a New Version of the XMS Server” on page 535**. **Do not continue with this procedure** unless you have been directed to do so by the Release Notes for this release or by Xirrus Customer Support.

2. Insert the XA-3300-CC installation CD into an available CD ROM drive. The CD’s autoplay feature starts the installation wizard automatically.
3. Click on the **Next** button to begin the installation process. When prompted, you must accept the Xirrus End User License Agreement.



Figure 7. Installation Wizard and End User License Agreement

4. Click on the **Next** button to continue the installation process. When prompted, you may click the **Choose** button to select a location where you want to install the application, or click on the **Restore Default Folder** button to select the default folder as the desired location. (Figure 8) The default folder is: C:\XA-3300-CC.



Figure 8. Choose an Install Location for the Application

5. Click on the **Next** button to continue the installation process.

At this point, a Windows Security Alert message may appear (Figure 9), informing you that Windows Firewall is blocking some features of Java. Click the **Unblock** button to allow correct installation and operation of XMS.



Figure 9. Unlocking Java

6. You must now define the ports that your server will use. (Figure 10) If the default ports provided by the installation wizard are already being used, enter new port assignments then click on the **Next** button. If you want to use the default ports, leave the port fields unchanged and click **Next**.



Figure 10. Setting Up the Ports



Port Usage - In addition to the ports configured above, the XMS server has requirements for other port assignments. Please see “**XMS Port Requirements**” on page 22 for details.

Many of these assignments are not configurable as part of the installation process. Please **do not modify** the assignments of non-configurable ports.

7. Review your installation parameters.



Figure 11. Reviewing Your Installation Parameters

8. If you are satisfied with the installation parameters you provided, click on **Install** to install the Xirrus Management System on your server. A progress window will be displayed while the installation process completes—it will take a few minutes. After a successful installation, click on the **Done** button.



Figure 12. Installation Completes

Proceed to the next chapter, **Getting Started with XMS**, to start using XMS.



Licensing - The XMS server requires a license for full operation. The license is entered via the client, and will automatically be requested the first time you start the client. Please see **“Licensing the XMS Server”** on page 35 for details.

Getting Started with XMS

This chapter describes how to get started using the XMS server and the XMS clients, regardless of whether you are running the XMS server on your own computer or on a Xirrus Management Appliance.

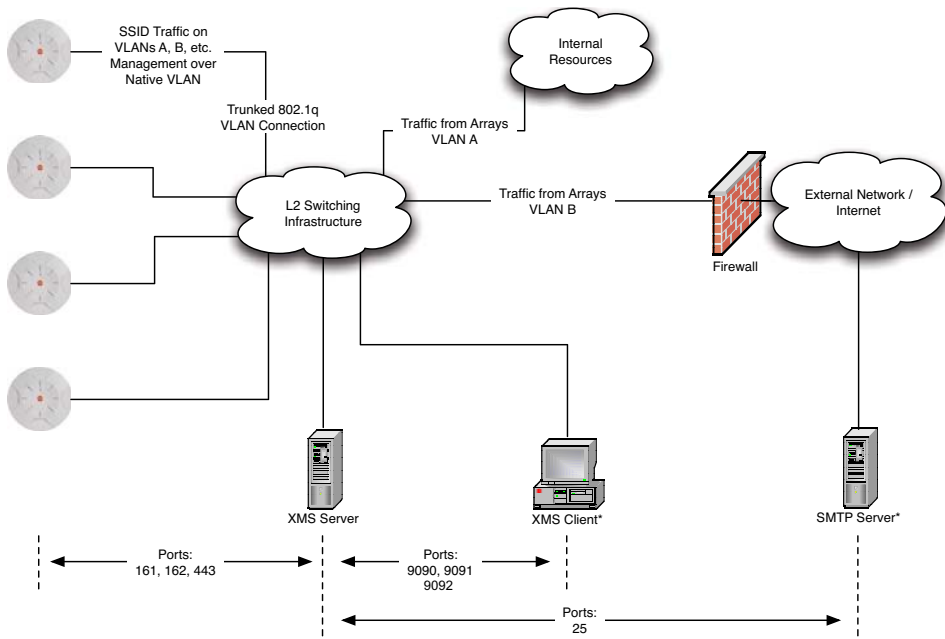
Section headings for this chapter include:

- **"XMS Port Requirements" on page 22**
- **"Starting and Managing the XMS Server" on page 25**
- **"Initial Server Setup for Linux-based Management Appliances" on page 28**
- **"Starting the XMS Client Interface" on page 29**
- **"Licensing the XMS Server" on page 35**
- **"Discovering Networks and Arrays" on page 37**
- **"Closing Down the Java Client Interface" on page 37**
- **"Shutting Down the XMS Server" on page 38**

XMS Port Requirements

A number of ports are used by XMS and by various Array features and must not be blocked by firewalls. The **Port Requirements table on page 23** lists ports and the features that require them. Note that Array port requirements are included in the table for your convenience—some of the Array ports shown are unrelated to communication with XMS. If you are using a feature, please make sure that the ports that it requires are not blocked by firewalls or other policies, and that they do not conflict with any other port assignments.

As an example, some XMS port requirements are illustrated in **Figure 13**. XMS requires ports 161, 162, and 443 to be passed between Arrays and the XMS server. Similarly, ports 9090, 9091, and 9092 are required for communication between the XMS server and XMS clients, and port 25 is typically used by the XMS server to access an SMTP server to send email notifications.



* XMS Client and SMTP Server may be internal or external resources.

Figure 13. Sample Port Requirements for XMS

The following table lists port requirements for the Array and for XMS, how they are used, and whether they may be changed.

Port	Application	Peer	Configurable
XMS			
22 tcp	SSH	Arrays	Yes
25 tcp	SMTP	Mail Server	Yes
161 udp	SNMP	Arrays	No
162 udp	SNMP Traphost 1	Arrays	Via XMS config file
514 udp	Resident Syslog server	Internal*	Via XMS config file
1099 tcp	RMI Registry	Internal*	No
2000 tcp	XMS Back-end Server	Internal*	No
2022 tcp	SSH	XM-3320/3340/3360	Yes
3306 tcp	MySQL Database	Internal*	No
8001 tcp	Status Viewer	Internal*	No
8007 tcp	Tomcat Shutdown	Internal*	During installation
8009 tcp	Web Container	Internal*	During installation
9090 tcp	XMS Webserver	XMS client	During installation
9091 tcp	XMS Client Server	XMS client	Via XMS config file
9092 tcp	XMS Client Server	XMS client	Via XMS config file
9443 tcp	XMS WMI SSL	XMS web client	No
* Internal to XMS Server, no ports need to be unblocked on other network devices			

Port	Application	Peer	Configurable
Array			
20 tcp 21 udp	FTP	Client	Yes
22 tcp	SSH	Client	Yes
23 tcp	Telnet	Client	Yes
25 tcp	SMTP	Mail Server	No
69 tcp	TFTP	TFTP Server	No
161 tcp/udp	SNMP	XMS Server	No
162 tcp/udp	SNMP Traphost Note - Up to four Traphosts may be configured.	XMS Server	Yes - but required by XMS
443 tcp	HTTPS (WMI,WPR)	Client	Yes
514 udp	Syslog	Syslog Server	No
1812, 1645 udp	RADIUS (some servers use 1645)	RADIUS Server	Yes
1813, 1646 udp	RADIUS Accounting (some servers still use 1646)	RADIUS Accounting Server	Yes
2055 udp	Netflow	Client	Yes
5000 tcp	Virtual Tunnel	VTUN Server	Yes

Starting and Managing the XMS Server

You may manage the XMS server using its management tools:

- “Managing XMS on Linux-based Management Appliances” on page 25
- “Managing XMS on Windows-based Servers” on page 27

NOTE: For full operation, the XMS server must have a license installed. See “Licensing the XMS Server” on page 35.

Managing XMS on Linux-based Management Appliances

On the XM-3320/3340/3360, the XMS server is started automatically when your computer is restarted. Use the browser-based XMS web client (**Figure 14**) to perform mandatory initial configuration, to restart or reboot the server, and for server maintenance.

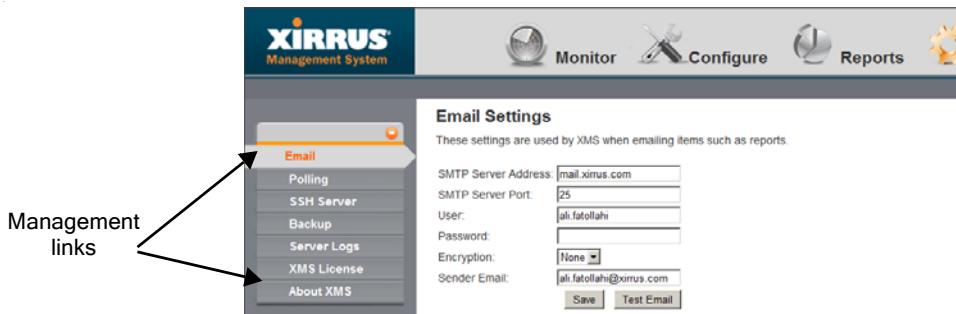


Figure 14. Server Management using the Web Client

NOTE: XMS web client access to the XMS server requires access to ports 9090 and 9443. Make sure that this port is open in any firewalls that exist between clients and the XMS server.

To access the web client, set your browser's URL to the XMS server machine's IP address or host/domain name, followed by **:9090**. For example, **http://192.168.10.40:9090**. When the splash page appears, click the **Web Client** button on the lower right.

Log in to the web client (the default for both fields is **admin**). In a few moments the web client Dashboard appears. Click the **Settings** button on the top, then click **Status** on the left to display the Status page. It shows a summary of server status. You will need to proceed to **"Initial Server Setup for Linux-based Management Appliances" on page 28** to perform required initial setup on the server.

*NOTE: You may use the Command Line Interface (CLI) to manage the XMS server via SSH. Access it at port 2022 and log in using **admin/admin**. Do **not** use port 22 for CLI.*

If XMS is not running properly, you may click the **Restart Application** button on the lower left to restart the XMS server software. If the server is currently running, an orderly shutdown will be performed first.

The **Reboot Appliance** button will reboot the Management Appliance—this will shut down XMS related processes in an orderly manner before rebooting. Rebooting and restarting will take about two minutes on a new Management Appliance. As XMS is used and the database grows, startup integrity checks will take longer. (For shutdown, see **"Shutting Down the XMS Server" on page 38**.)

Managing XMS on Windows-based Servers

The XMS server is started automatically when the XM-3300 is restarted.

Alternatively, you may start the XMS server using the Xirrus Server Management Tool (XSMT). XSMT is used to start, stop, or view the status of the server. To start XSMT, use the Windows **Start** button > **All Programs** > **Xirrus** > **Xirrus Management System** > **XA-3300-CC**. The Server Console window is displayed, and then the XSMT window. When the **Start** button (at the bottom of the XMS Server Manager tab of XSMT) is enabled, click it to start the server.

During the server initialization process, the XSMT Logs panel displays high-level progress messages, and the Server Console displays detailed messages.

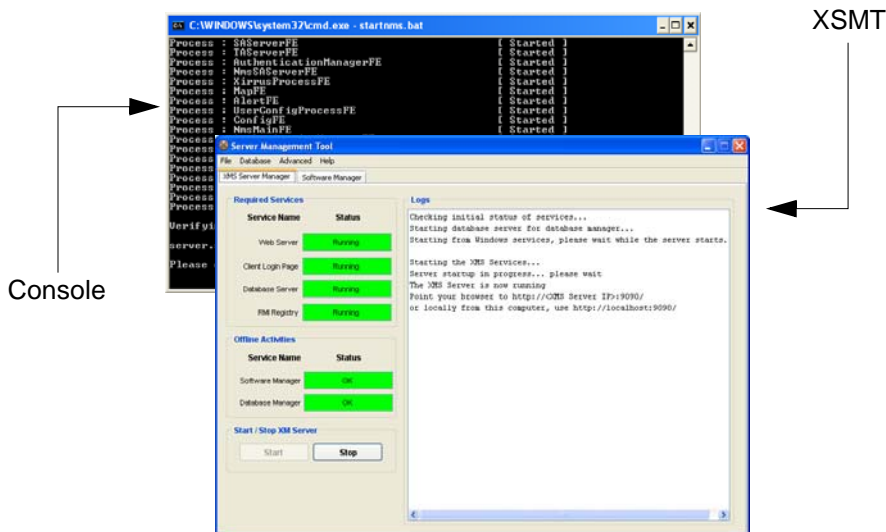


Figure 15. XSMT Window, Showing Typical Running Status

During the installation process, there are options to have XSMT start the XMS server automatically, or to wait for the administrator to explicitly start it. If all four Required Services indicators do not turn green, you may start the XMS server by clicking the **Start** button on the lower left when XSMT enables it.

When XMS server startup is finished, the XMS Server Manager tab of XSMT will indicate that the server is up and running. **Figure 15** shows an example of a successful server initialization process. The state of the topmost three servers is **Running**, and they are shown in green.

When the XMS server is ready for clients to be started, the Logs section on the right of the window will display:

```
*** The XMS Server is now running
Point your browser to http://<XMS Server IP>:9090/
or locally from this computer, use http://localhost:9090/
```

When the server starts for the first time, it will initialize the database. To add your Xirrus Arrays to the XMS database, please see **“Discovering the Network” on page 67**.

For more information on using XSMT, see **“Managing XMS on Windows-based Systems” on page 523**.

***NOTE:** The XMS server does not have a default backup schedule, so it is **very important** for you to create a backup schedule after installation. After you start an XMS client, see **“Backup Manager” on page 499**.*

Initial Server Setup for Linux-based Management Appliances

Use the XMS web client to complete the following steps on the XM-3320/XM-3340/XM-3360 in order to configure XMS for proper operation.

When you start the XMS server for the first time, you must configure the following settings as described in **“Initial Server Setup” on page 504**.

- Network Settings
- Date/Time Settings
- Database Backup Settings

When those steps are complete, proceed to:

- Start an XMS Java client (next section), then start **“Discovering the Network” on page 67**.

- Set the XMS polling interval based on your deployment size (see **“Web Client — Polling Settings”** on page 516 or **“XSMT - Advanced Settings”** on page 537)

Important! The XMS server does not have a default backup schedule, so you must create one after installation.

Starting the XMS Client Interface

XMS has two browser-based client interfaces with somewhat different capabilities:

- The Java Client includes a full set of management capabilities for your Wi-Fi network. The Dashboard provides an at-a-glance overview of the health of your network; network discovery may be fine-tuned; contour maps display the RF coverage provided by your Arrays; alarms and events are displayed; pages for Arrays, IAPs, Stations, and SSIDs show detailed information and allow configuration; rogue devices are monitored; and Array configuration policies may be configured.
- The Web Client is a very fast and efficient application for viewing the status of your network and performing certain network management tasks. It does not have all of the same features as the Java client, but it does have some extended features that are only available on this client. In particular, bulk editing allows you to quickly configure selected identical settings on a number of Arrays in one step. Reports on system performance may be created. Additional XMS server administration functions are available in the web client, especially for Linux-based servers.

This section describes how to start the Java client. To start and use the web client, please see **“The XMS Web Client”** on page 423.

XMS Java Client—Minimum System Requirements

- Java-enabled Web browser
- Java Version 6
- Monitor (1280 x 1024 or better); keyboard and mouse

Please check your Release Notes for the latest requirements.

To run the Java client, XMS client machines require a Java-enabled Web browser to connect with the server. Once a connection is established with the server, all client-related files are downloaded to the local machine. Download time depends on machine capability and available bandwidth.

The client machine must have Java 6 installed. If Java 6 is not present, the user's browser will display an error message. Some browsers will prompt the user to download required software (but may not necessarily identify the download target as being Java 6). If necessary, the user may download the Java runtime from <http://java.sun.com/javase/downloads/index.jsp>; a link to the web site will be provided with the warning to the user. Use the Java® Runtime Environment (JRE), version 6.0 or higher.

Java Client

The XMS Java client requires a Java-enabled Web browser to connect with the XMS server running on a remote machine. The first time that a client machine establishes a connection with the server, a Web Start client is downloaded to the local machine. This installs an XMS icon on the local desktop. Clicking this icon provides the fastest way to start the XMS client for future connections to the server. This is described in the following procedures.

- **Starting the XMS client for the first time**
- **Starting the Java client after the first time.**

When the user connects to the XMS server, an error will occur if Java is not present. If necessary, the user may download Java from <http://java.sun.com/javase/downloads/index.jsp>. Use the Java® Runtime Environment (JRE), version 6.0 or higher.

NOTE: XMS will not necessarily warn you if you have an older version of JRE installed. Please make sure that you have JRE 6 installed on all client computers.

Note: Client access to the XMS server requires access to ports 9090, 9091, and 9092. Make sure that these ports are open in any firewalls that exist between clients and the XMS server.

Starting the XMS client for the first time

1. To install the XMS Web Start client from a remote workstation, point your workstation's browser to the IP address or hostname for the XMS server machine followed by :9090. For example, if the IP address is 192.168.10.40, point your browser to **http://192.168.10.40:9090**.

The XMS Start window appears. (Figure 16)



Figure 16. XMS Start Window

2. Click the **Java Client** button.

Some browsers may ask you to choose whether to open or save a file named **xms256.jnlp**. Select **Open with** (use the suggested application, Java Web Start Launcher) and click **OK**.

3. If you have not previously accessed this XMS server you may see a security warning, with the Publisher identified as Xirrus. (Figure 17—the message may vary depending on the browser in use.) Check the box labeled **Always trust content from this publisher** and click **Run**.

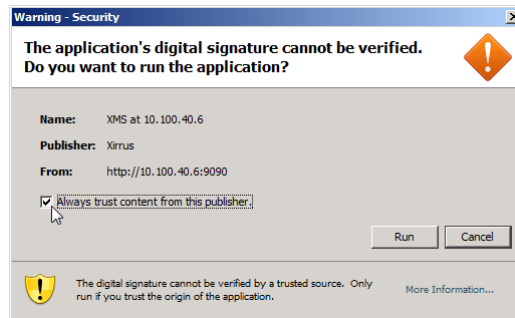


Figure 17. Web Start Client Security Warning

4. The XMS Login dialog appears. Log in to the client interface using the default username and password (the factory default for both fields is **admin**). Click **Connect**.

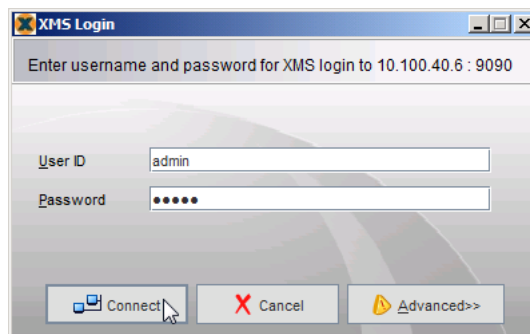


Figure 18. Client Login Window (Browser)

It will take a few moments for Java to start the client interface.

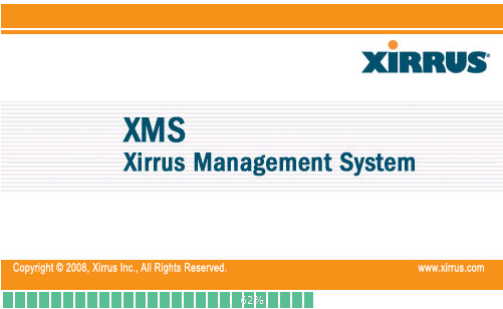


Figure 19. Loading the XMS Client

When the client has started, you are presented with the XMS client’s Dashboard window—this is the default start-up view.

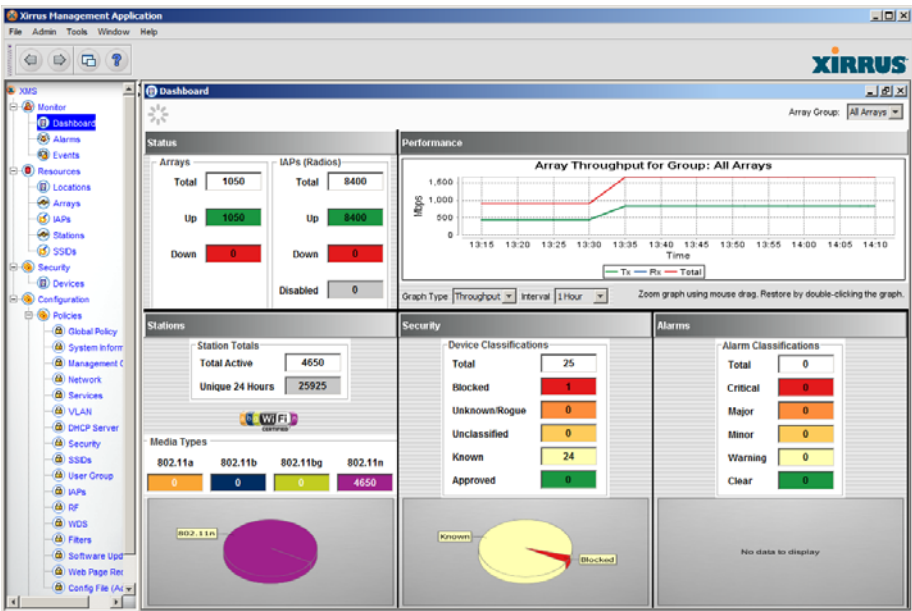


Figure 20. The Dashboard - XMS Java Client Window

NOTE: For full operation, the XMS server must have a valid license installed. Otherwise, the current license is displayed along with the client. See “[Licensing the XMS Server](#)” on page 35.

Starting the Java client after the first time

When you first install the XMS Web Start client as described in [Starting the XMS client for the first time](#), an icon is placed on your desktop. ([Figure 21](#)) This icon allows you to quickly start the XMS client.

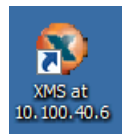


Figure 21. XMS Web Start Client Icon on desktop

1. Click the XMS Web Start client icon.
2. The XMS Login dialog appears. Log in to the client interface using the default username and password (the factory default for both fields is **admin**). Click **Connect**.

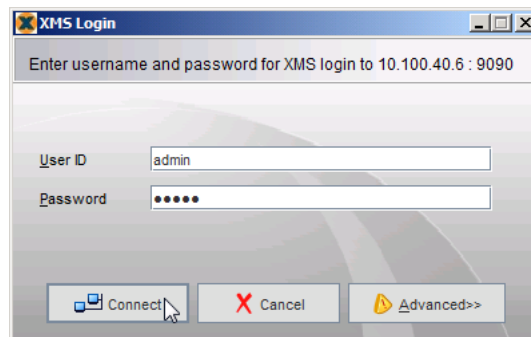


Figure 22. Client Login Window (Browser)

It will take a few moments for Java to start the XMS client. When the client has started, you are presented with XMS’s Dashboard window ([Figure 20](#)).

Licensing the XMS Server



This section describes the license to use the XMS server. If you are looking for information regarding using XMS to manage Array licenses, please see “Managing Array Licenses” on page 189.

For full operation, the XMS server must have a license installed. Until the license is installed, the server will operate in a default mode that allows it to manage only one Array. Thus, without an appropriate license, **Discovery** will stop at one Array and will not allow more Arrays to be added. If you do not have a valid license, you will be notified each time you start an XMS client.



Valid XMS licenses are typically for a particular number of Arrays. When XMS has discovered the maximum permitted number of Arrays, no additional Arrays will be discovered.

Use the following steps to enter your license.

1. In the **Menu Bar** of the XMS Java client, select **Tools > Xirrus XMS License**. The Server License dialog box appears. (To license the server using the web client instead, please see “**Web Client—Managing the XMS Server License**” on page 520.)

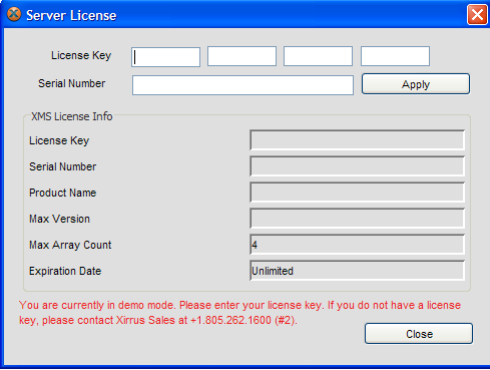


Figure 23. XMS Server License

2. Xirrus will supply you with a **License Key** and **Serial Number** for your server. Enter **both** of these fields exactly as they were provided to you (the fields are not case-sensitive), and click **Apply**.
3. After processing the license information, the following additional fields will be shown:
 - Product Name—XMS server’s product name.
 - Max Version—the highest release number supported by this license. All incremental upgrades to the release shown are also supported. For example, if Max Version is 5.0, then this license will run Release 5.0.999, but Release 5.1 will require an updated license.
 - Max Array Count—the server is licensed to manage a specific maximum number of Arrays. To manage additional Arrays, please contact Xirrus to upgrade your license.
 - Expiration Date—the date that this license expires.

Discovering Networks and Arrays

After completing a successful installation of XMS you will need to discover any reachable networks and Arrays, then decide which ones you want to manage from XMS.

XMS does not automatically discover any networks when it is first started. When the XMS Java client is started and there are no Arrays in the database, a popup dialog will direct the user to use discovery to add networks.

The procedures for discovering, adding, modifying and deleting networks and Arrays are covered in **“Discovering the Network” on page 67.**

Closing Down the Java Client Interface

To close down the Java client interface, click on the File button in the **Menu Bar** then choose **Exit**. Alternatively, you can simply click on the X button in the top right corner of the client interface. In either case, the system prompts you for a confirmation that you want to exit the client.

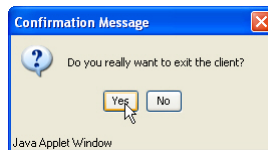


Figure 24. Closing Down the Java Client Interface

To exit the client, choose **Yes** when prompted.

- ! *Never turn off any Management Appliance at the power switch until you have closed down all applications, closed down the client interface, and stopped the server.*

Shutting Down the XMS Server

There is a correct way and an incorrect way to shut down the XMS server. Shutting down the server incorrectly can cause problems the next time you start XMS. If you need to shut down the server, you must use the following procedure:

1. Terminate all applications—see [Closing Down the Java Client Interface](#).
2. For Linux-based servers—in the **Status** page of the XMS web client, click the **Shutdown Appliance** button at the bottom of the window.

For Windows-based servers—click the **Stop** button in the **XMS Server Manager** tab of the Xirrus Server Management Tool (XSMT). When prompted, enter your password. The default username and password are both **admin** (all lowercase). See [“XSMT - Shutting Down the XMS Server” on page 531](#) for more information.

3. You will be notified when the server has shut down successfully. Note that on Linux-based systems the database server will be shut down as well. On Windows-based systems it will remain running—this is not a problem.
4. When the XMS server has shutdown successfully you may shut down your computer.

The XMS Java Client Interface

This chapter provides an overview of using the XMS Java client interface, which is a convenient tool for managing and configuring your multi-Array Wi-Fi network.

XMS also provides a Web Client interface, which offers a subset of the functions provided by the Java client, plus additional XMS server administration functions (especially for Linux-based management Appliances). The current chapter discusses usage of the Java client. For more information about using the XMS web client instead, please see the chapter titled **“The XMS Web Client” on page 423**.

The XMS Java client interface allows you to browse through the discovered Wi-Fi Arrays in your network, view network and device information, establish operating policies for individual Arrays or groups of Arrays, monitor the performance of all devices residing in the network, detect and monitor rogue AP devices, and identify problems. Section headings for this chapter include:

- **“Major Components of the Client Work Space” on page 40**
- **“Basic Window Operations” on page 53**
- **“Basic Table Operations” on page 57**
- **“Searching for Events” on page 64**
- **“Keyboard Shortcuts” on page 65**

To start the client, please see **“Starting the XMS Client Interface” on page 29**.

About the Images Shown in this Chapter

Most of the images provided as examples in this chapter are shown with the content of the Java client interface set at its factory default state. This is to maintain a consistent look, because the windows and tools can change depending on which operation you are performing and at what level (entire network, individual Array, or group of Arrays).

Major Components of the Client Work Space

Figure 25 highlights the locations of major components within the XMS Java client work space. Click on any callout in the following graphic to jump to a description of the selected component.

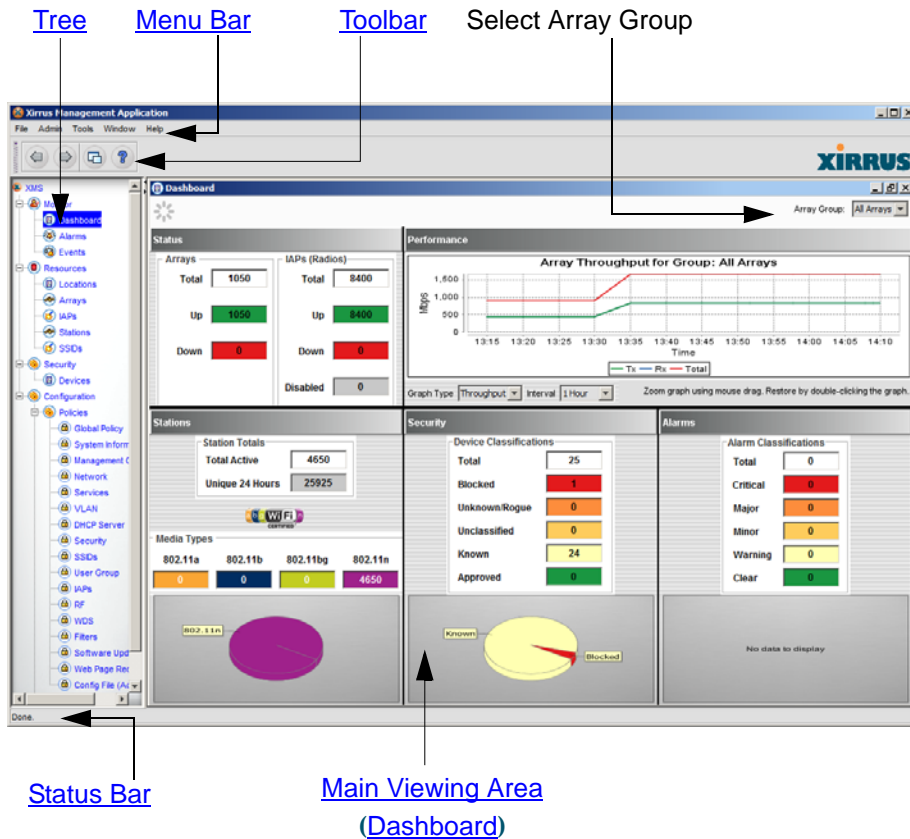


Figure 25. XMS Java Client Work Space

Menu Bar

The menu bar is located at the top of the Java client work space. Each menu item has its own set of functions and commands that appear in the form of a pull-down list when you click on a menu item. The content of the menu bar will change from window to window based on the functions you are using and the user privileges that have been assigned to you.

Figure 26 shows the menu items with their associated pull-down lists when you view the **Arrays** window.

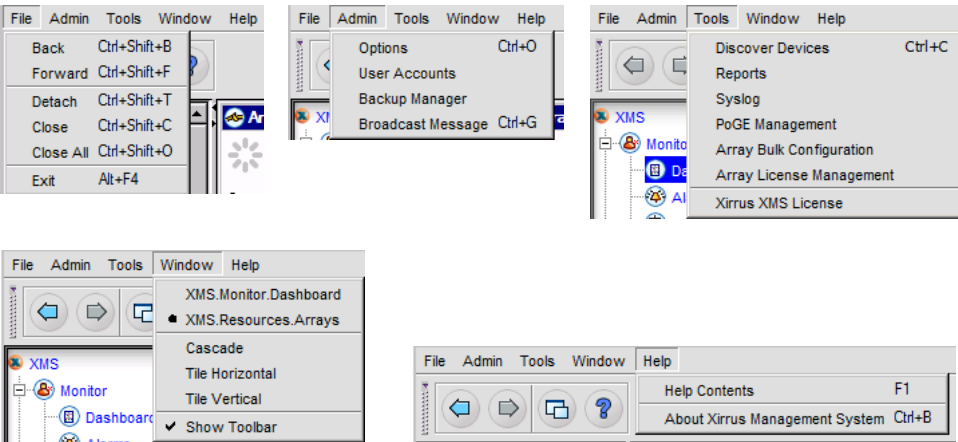


Figure 26. Java Client Menu Bar

Toolbar

The toolbar is located immediately below the **Menu Bar**. (**Figure 27**) Mouse-over **Tool Tips** are provided for all toolbar buttons, indicating the operation performed by each button.

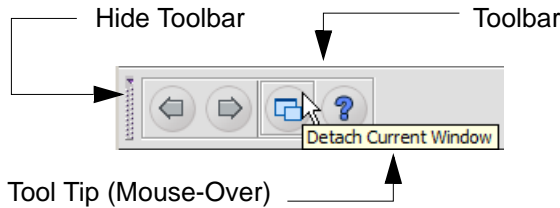


Figure 27. Toolbar (Default Map View)

Toolbar Buttons

The following buttons are available in the toolbar—from left to right:



Hide/Show Toolbar

Hide or show the toolbar. Hiding or showing the toolbar is a matter of personal preference. The default is to have the toolbar visible.



Go Back to Previous

Go back to the previously viewed window—only applicable if you have accessed more than one window.



Go Forward to Next

Allows you to toggle between the previously viewed window and the next window—only applicable if you have accessed more than one window and want to move forward to the next window.



Detach Current Window

Detaches the current window from the **Main Viewing Area** and manipulate the window independently of the client interface.



Help

Provides access to the XMS online help system.

Tree

Located at the upper left side of the client interface, the tree shows a hierarchical set of functional areas within XMS—built on a parent/child relationship of nodes. For example, in **Figure 28** the **Policies** node is considered the child to its upper level parent, **Configuration**.

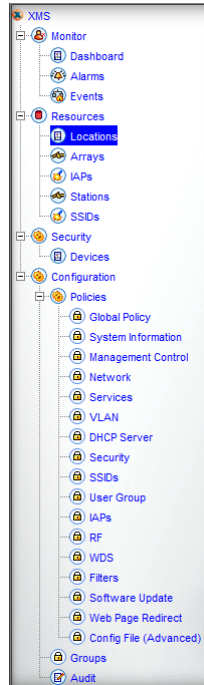


Figure 28. Tree (Expanded)

When you log in to XMS's client interface, the default view displayed in the **Main Viewing Area** is always the **Dashboard** (see **"Using the Dashboard" on page 91**). Clicking any node in the tree generates a new window corresponding to the item you selected. Any new windows you open don't replace existing windows. However, you can customize how your windows are displayed (for example, sizing, tiling and cascading). For information about how to display and organize your windows, see **"Basic Window Operations" on page 53**.

You can expand or collapse tree nodes, as desired. In addition, the frame that the tree resides in can be stretched either horizontally or vertically, which is useful as the tree grows or where the naming convention for a node is too long to be displayed in its entirety.

Status Bar

Located at the bottom of the client interface, the Status Bar provides the current status of any active system processes. For example, when a process is still in progress the Status Bar displays the **loading...** message. When a process has completed its task, the message displayed in the Status Bar is **Done**.



Figure 29. Status Message

Tool Tips

Tool tips are a standard feature that helps users navigate through any client or application interface. They provide a convenient way of identifying components within the interface and are activated by rolling your mouse pointer over an item (no clicking is involved).

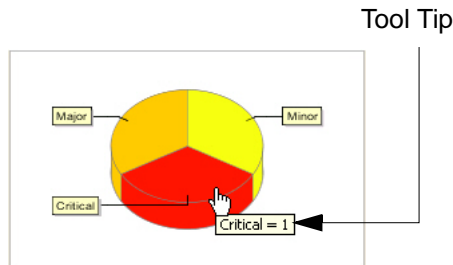


Figure 30. Tool Tips

The vast majority of elements displayed by XMS's client interface are supported with tool tips. To reveal a tool tip, simply roll your mouse pointer over the area of interest.

Other Navigation Tools

In addition to the navigation tools already discussed, the XMS client interface supports task menus that are generated by right-clicking on elements within the interface, and keyboard shortcuts.

Right-Click Menus

In keeping with standard Windows navigation techniques, you can generate context-sensitive menus by right-clicking on objects and other elements within the client interface, for example, map symbols and management windows within the tree. **Figure 31** shows an example of menus generated by right-clicking on an Array after selecting multiple entries in the **Arrays** window.

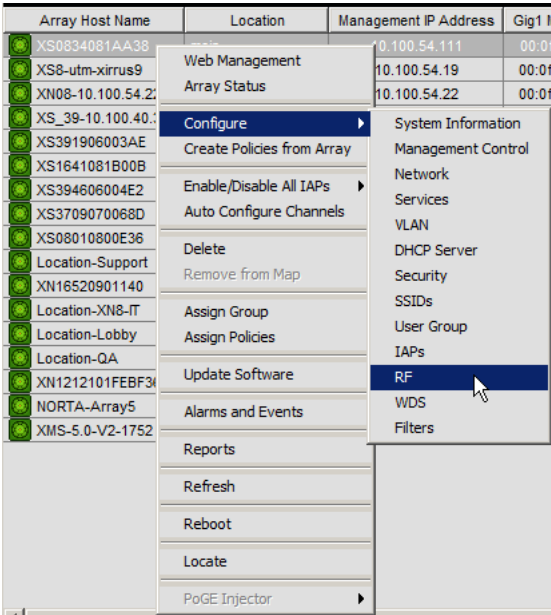


Figure 31. Right-Click Menus (Arrays Window)

Some tables allow you to select multiple entries. The action you select from the right-click menu will be applied to all selected entries sequentially, if possible. Use **Ctrl+Click** to select additional entries, or **Shift+Click** to select a range of entries.

Keyboard Shortcuts

Keyboard shortcuts are useful for experienced users who want to access, monitor or manage their network more quickly than a typical mouse allows. Be aware that some shortcuts are the same but invoke different commands depending on which window is the active window. For a listing of keyboard shortcuts that are available with the client interface, go to **“Keyboard Shortcuts” on page 65**.

Main Viewing Area

The Main Viewing Area is shown in **Figure 32** as the BLUE area—depicted here for clarity with no active windows. It is in this area that all management windows are displayed, with the exception of pop-ups. The default state for this area (when you log in) is to show the **Dashboard**. Another useful window is the **main Location Window**.

Whenever you click on an item in the **Tree**, the associated window is displayed in the Main Viewing Area, but you have the option of detaching any window from this area so that the window can be manipulated independently of the client. For more information about windows and how you can use them to best suit your needs, see **“Basic Window Operations” on page 53**.

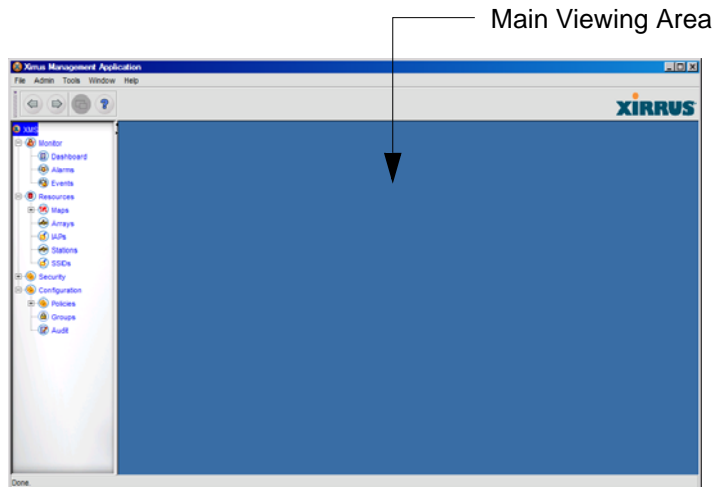


Figure 32. Main Viewing Area

Monitoring Windows

These monitoring windows are generated by clicking on items that reside under the parent **Monitoring** function in the **Tree**, with the selected child window(s) being displayed in the **Main Viewing Area** of the client interface.

Monitoring windows include:

- **Dashboard**
- **Events**
- **Alarms**

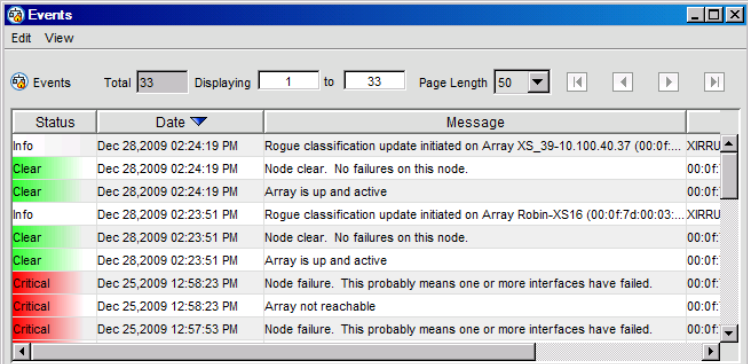
***NOTE:** Access the **Syslog Events** window from the menu, by selecting **Tools> Syslog**.*

Dashboard

The dashboard is the main user interface of XMS, designed to give you an overview of all aspects of the functioning of your Array network on one window. The Dashboard is discussed in detail in **“Using the Dashboard” on page 91**.

Other Monitoring Windows

Figure 33 shows an example of the Events window—detached from the client interface for clarity. From this window you can choose to view data about all network events displayed in the list or select specific events and view the data associated with the selected event only. The data available to you in any monitoring window is determined by which window in the **Tree** you open.



Status	Date	Message
Info	Dec 28, 2009 02:24:19 PM	Rogue classification update initiated on Array XS_39-10.100.40.37 (00:0f:...
Clear	Dec 28, 2009 02:24:19 PM	Node clear. No failures on this node.
Clear	Dec 28, 2009 02:24:19 PM	Array is up and active
Info	Dec 28, 2009 02:23:51 PM	Rogue classification update initiated on Array Robin-XS16 (00:0f:7d:00:03:...
Clear	Dec 28, 2009 02:23:51 PM	Node clear. No failures on this node.
Clear	Dec 28, 2009 02:23:51 PM	Array is up and active
Critical	Dec 25, 2009 12:58:23 PM	Node failure. This probably means one or more interfaces have failed.
Critical	Dec 25, 2009 12:58:23 PM	Array not reachable
Critical	Dec 25, 2009 12:57:53 PM	Node failure. This probably means one or more interfaces have failed.

Figure 33. Monitoring Window (Events)

Resource Windows

These management windows are generated by clicking on items that reside under the parent **Resources** function in the **Tree**, with the selected child window(s) being displayed in the **Main Viewing Area** of the client interface. Resource windows include:

- **Locations**
- **Arrays**
- **IAPs**
- **Stations**
- **SSIDs**

Location Window

This is the window where your maps are displayed. (**Figure 34**)

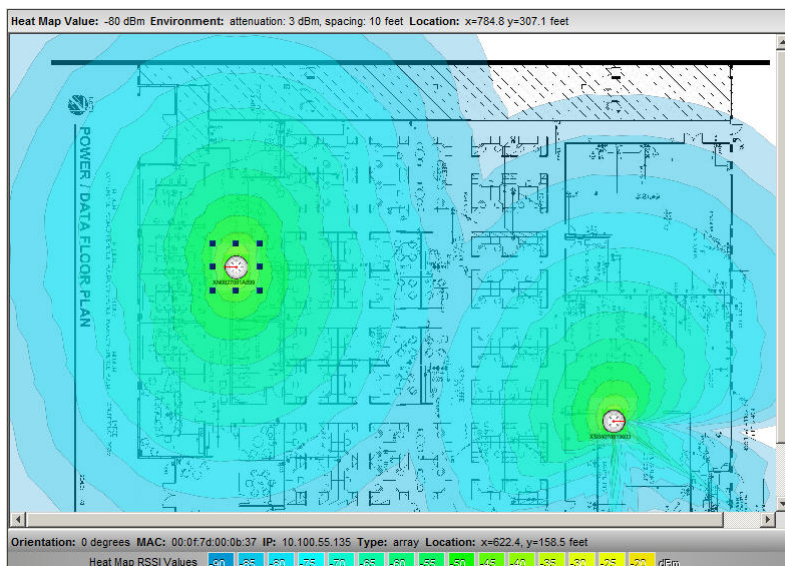


Figure 34. Location (Map) Window

The client interface allows you to create custom maps. To create a custom map, go to **“Adding a New Map”** on page 144.

Other Resource Windows

Figure 35 shows an example of the Arrays window—detached from the client interface for clarity. From this window you can choose to view data about all Arrays displayed in the list or select specific Arrays and view the data associated with the selected Arrays only. The data available to you in any resource window is determined by which window in the **Tree** you open.

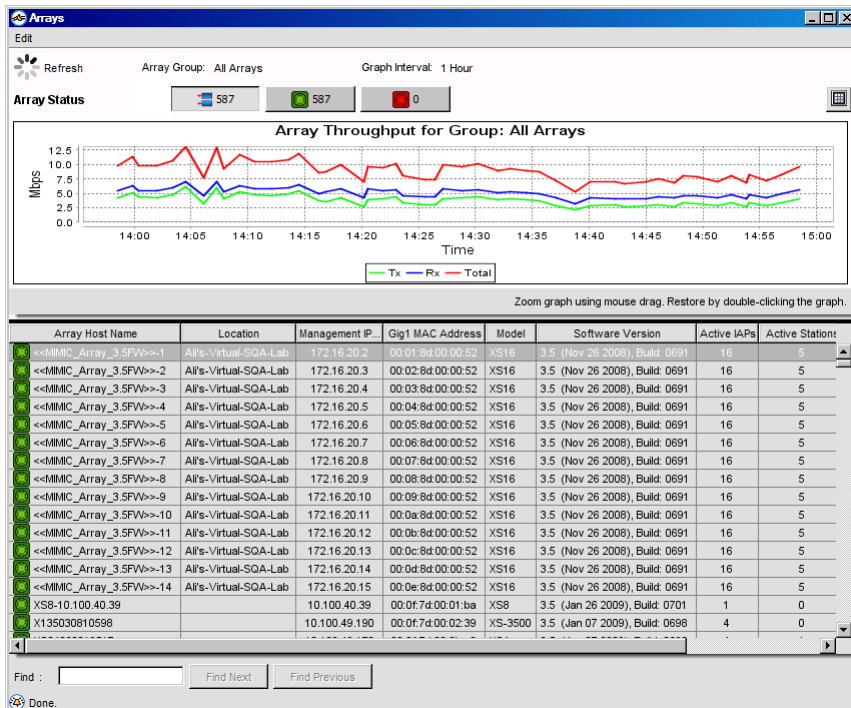


Figure 35. Resources Window (Arrays)

Security Window

This section of the tree offers one window—**The Devices Window**, designed to all the rogue APs detected by your Array network. You may then classify these devices according to whether they present a threat or not.

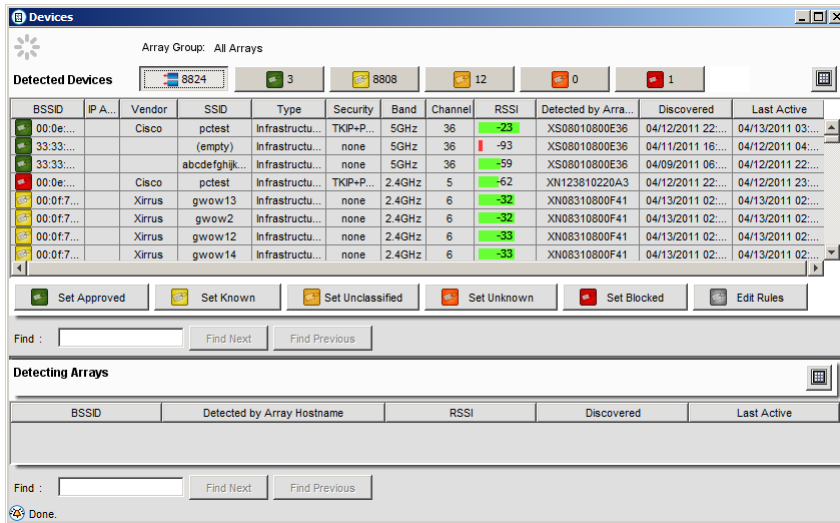


Figure 36. Security Window

Configuration Windows

The management policy windows are generated by clicking on items that reside under the parent **Configuration** function in the **Tree**, with the selected child window(s) being displayed in the **Main Viewing Area** of the client interface.

Configuration windows for policies include:

Policies:

- **Global Policy**
- **System Information**
- **Management Control**
- **Network**
- **SSIDs**
- **User Groups**
- **IAPs**
- **RF**

- Services
- VLAN
- DHCP Server
- Security
- Configuration File (Advanced)
- WDS
- Filters
- Software Update
- Web Page Redirect (WPR)

Other configuration items

- Groups
- Audit

Figure 37 shows an example of the Security Policy window—detached from the client interface for clarity. From this window you can choose to view the details for a selected policy, add a new policy or modify an existing policy. The data available to you in any configuration window is determined by which window in the **Tree** you open.

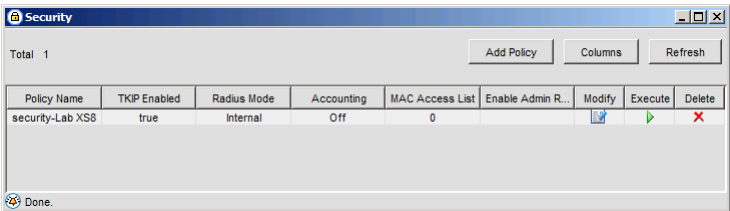


Figure 37. Configuration Window (Security Policy)

XMS Administration Windows

XMS administration functions are accessed via the **Admin** menu on the **Menu Bar** rather than through the Tree. They open independent, detached windows rather than opening windows in the **Main Viewing Area**. The following functions are available from the **Admin** menu:

- **Options (Country of Operation)**—sets the Country in which the Arrays are operating.
- **User Accounts**—manages user accounts.
- **Backup Manager**—manages the XMS Database.
- **Broadcast Message**—broadcasts a message to all users.

Backup Manager

The **Backup Manager** window is accessed from the **Admin** menu.

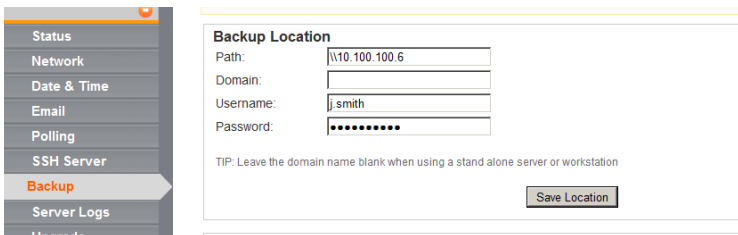


Figure 38. Backup Manager

Its main functions are:

- Configure the scheduling of your database backups on a daily, weekly or monthly basis.
- Perform a backup of the database on demand (immediate).
- Restore the database from a backup file.

It is recommended that you create database backups regularly, and backup on demand after implementing many changes within the client interface. Backups generally take just a few seconds to complete. **Figure 38** shows the Backup Manager window.

For more information about database administration, see **“XMS Administration” on page 495**.

Basic Window Operations

This section describes some of the basic operations that can be performed with client windows. The procedures documented here assume that you are using the mouse to navigate through the client. If you are an advanced user and prefer to use **Keyboard Shortcuts**, this method will yield the same results; however, Xirrus does not accept responsibility for errors made by inexperienced users who choose to use shortcuts.

Navigating through Active Windows

When multiple windows are open in the **Main Viewing Area**, you can move forward to the next active window or move back to the previous window.

Moving Forward

To move forward to the next window, either click on the **Go Forward to Next** button in the **Toolbar** or go to **File** in the **Menu Bar** and choose **Forward**.

Moving Back

To move back to the previous window, either click on the **Go Back to Previous** button in the **Toolbar** or go to **File** in the **Menu Bar** and choose **Back**.

Detaching a Window from the Client

Sometimes you may want to detach a window from the client. For example, if you want to create a snapshot of the window using the **Fn+Print Screen** function in Windows, the window must be detached (otherwise the entire client interface will be captured). Detaching windows can also be useful for your own organizational purposes.

To detach a window from the **Main Viewing Area** and view it as a separate window, either click on the **Detach Current Window** button in the **Toolbar** or go to **File** in the **Menu Bar** and choose **Detach**.

Re-Attaching a Window

Windows are never permanently detached from the client, so a re-attach button does not exist. To see a detached window return to the **Main Viewing Area**, simply click on the **✕** button in the top right corner of the detached window.

Minimizing and Maximizing Windows

Similar to a standard Windows environment, you can minimize or maximize windows within the **Main Viewing Area**. All minimized windows are stored within the client (not on your desktop).

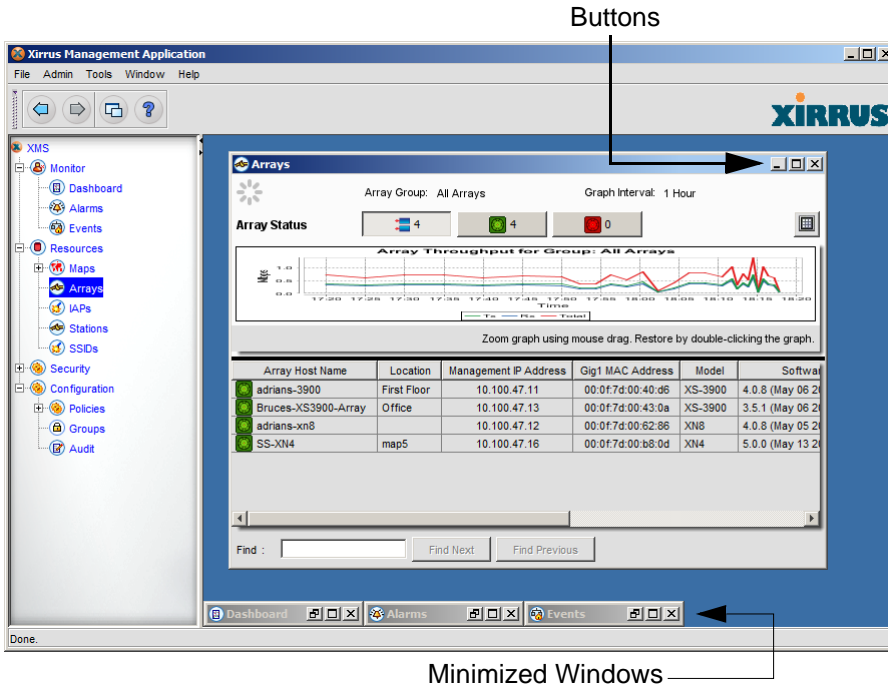


Figure 39. Minimized Windows



Click on this button to minimize windows.



Click on this button to maximize windows.

Arranging Windows

When multiple windows are open you can arrange for the windows to tile horizontally or vertically (next to each other) when displayed, or arrange for the windows to be displayed as cascading windows (overlapping). **Figure 40** shows an example of three open windows arranged with the horizontal tiling option.

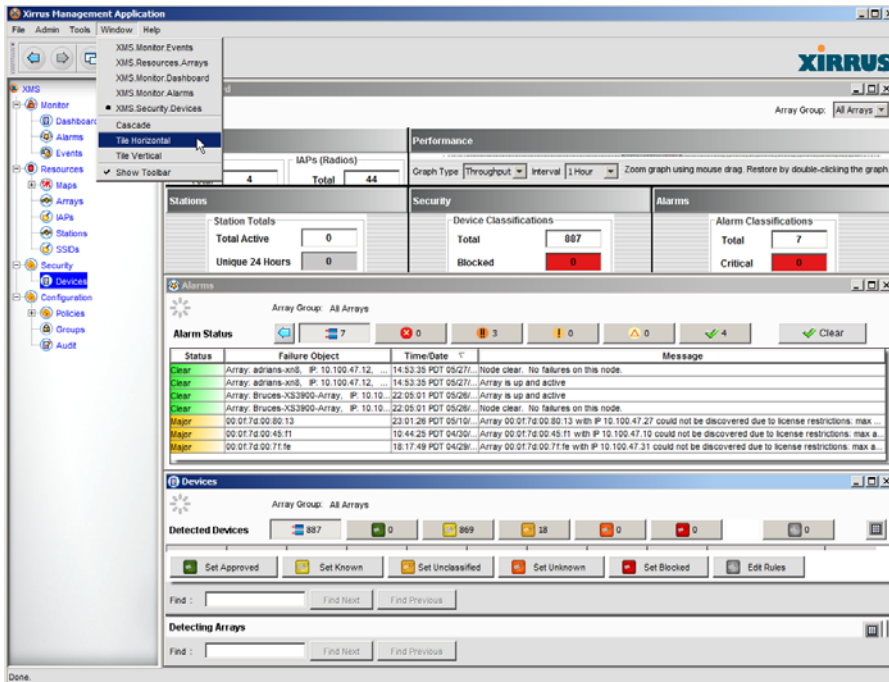


Figure 40. Horizontal Tiling of Windows

To arrange your open client windows, go to **Window** in the **Menu Bar** and choose one of the following:

- Cascade
- Tile Horizontal
- Tile Vertical

Closing a Window

You have the option of closing just the active window or closing all open windows.

Closing the Active Window

To close just the active window, go to **File** in the **Menu Bar** and choose **Close**. You can also close an active window by clicking on the **✕** button in the top right corner of the window.

Closing All Open Windows

To close all open window, go to **File** in the **Menu Bar** and choose **Close All**.

Basic Table Operations

Some of the XMS windows include a table with data retrieved from the XMS database. For example, if you select **Events** under the **Monitoring** function, the Events window is displayed in the **Main Viewing Area** as a table.

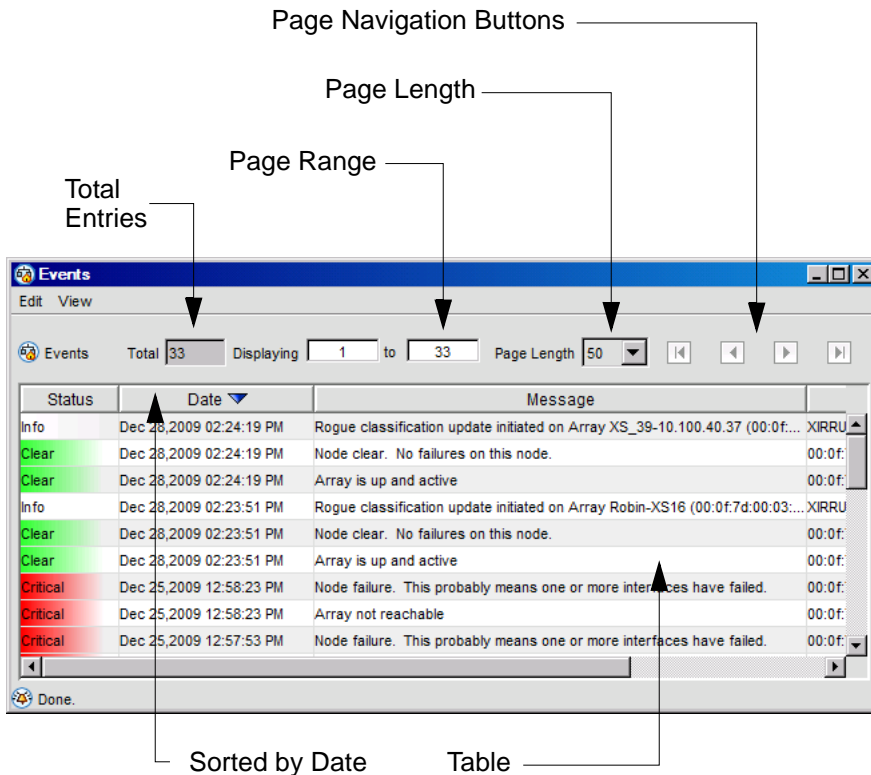



Figure 41. Typical Table (Events)

Note that at times, tables may show only selected items. For example, you may have:

- Selected a particular **Array Group** in the **Dashboard**. (See **“About Dashboard Data” on page 92**).
- Clicked a button in a status bar. For example, click  in the **Alarms Window** to see all critical alarms.

- Clicked on a particular type of alarm in the **Dashboard**.
- Filtered the list by **Searching for Events**.

The method for restoring the table to show all entries varies:

- If a table like the Events table is showing only your search result entries, the **Show All** button will appear at the top right of the window. Click it to return to viewing all entries.

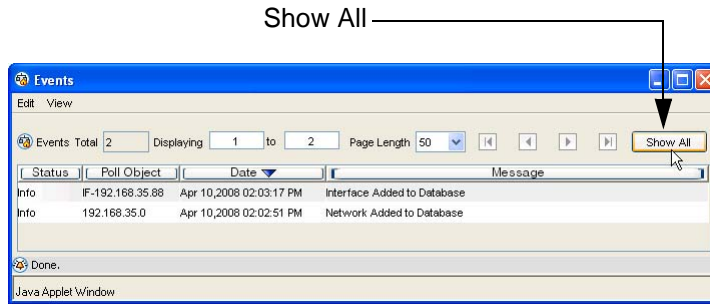



Figure 42. Show All Events After a Search

- Tables in other windows, like the **Arrays** window, may be filtered by clicking one of the buttons in a status bar at the top of the window. To return to viewing all entries in those windows, click the Total button on the status bar.  You can also use the counts displayed in the status bar to determine whether entries are being filtered.
- Tables in resource windows, like the **Arrays** and **IAPs** windows, may be filtered by selecting an Array Group in the **Dashboard**. The Array Group is displayed on the upper left. To return to viewing all entries, go to the Dashboard window and set the **Array Group** field on the upper right to **All Arrays**.

Page Navigation Buttons

Some tables, like the Events window, display a set number of entries per page. The page navigation buttons shown in [Figure 41](#) are grayed out (not available) unless the table contains more than one page of information. In this case, these buttons become active and allow you to navigate through multiple pages in the following ways (from left to right):

- **First Page**
Go to the first page of the table.
- **Previous Page**
Go to the previously viewed page in the table.
- **Next Page**
Go to the next page in the table.
- **Last Page**
Go to the last page in the table.

Setting the Page Length for a Table

To change the maximum number of rows that will be displayed on each page of a table, choose a value from the Page Length pull-down list (either 50, 100, 250, 500 or 1000). The default is 50 rows per page.

Refreshing the Page View

To refresh the data in a table, go to **View** in the [Menu Bar](#) and choose **Refresh**, or right-click in any row and choose **Refresh** from the pull-down list. All data in the active table is updated to the latest values.

Specifying a Range

To view data based on a specific range of rows, enter a value for the first row to be displayed in the **Displaying** field then enter value for the last row to be displayed in the **to** field. When finished, press the **Enter** key to refresh the table so that only the rows you specified are included in the table. The maximum number of visible rows when a table window is maximized is 36, although the table may contain many more rows than the window can display. Specifying a range defines how many rows the table contains (not how many rows it can display in the window).

Sorting Table Details

You can sort the data in a table based on the column type, and the details can be viewed either in ascending or descending order. The type of sorting (ascending or descending) is indicated by **Up** and **Down** arrows in the column header, where applicable. Where arrows appear in a column header, simply click the header to toggle the sorting sequence between ascending and descending. The sorting operation can be performed on the server side or the client side.

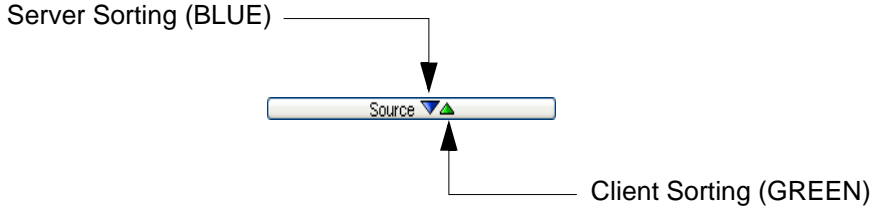


Figure 43. Table Sorting Arrows

Server Level Sorting

Sorting tables at the server level sorts all data in XMS and is not restricted to just the data available in the client interface. For example, if there are 100 events logged by XMS and only 50 are displayed in the client, sorting at the server level sorts all 100 events and not just the 50 events that are displayed. The default is for all sorting to be performed at XMS server level. Server level sorting is indicated by a BLUE arrow (ascending or descending) in the column header and is performed by clicking inside the header.

Client Level Sorting

Sorting tables at the client level sorts only the data currently displayed in the client interface. For example, if there are 25 events displayed in the client but 300 events stored in the XMS database, sorting at the client level sorts just the 25 displayed events and not the entire 300 events in the database. Client level sorting is indicated by a GREEN arrow (ascending or descending) in the column header and can only be performed by pressing the **Ctrl** key while clicking inside the header. If you don't press the Ctrl key, then all sorting is always performed at the server level.

Searching for Table Entries

Some tables have a Find field underneath the table, and they are used as follows. (If the window has no Find field, like the Events, Syslog, SSIDs, and Audit windows, search as described in “Searching for Events” on page 64.) Enter a string in the **Find** field, and XMS will search for the first matching entry in the table as you type the string. Click **Find Next** or **Find Previous** to find additional matching entries. If the Find field turns red, then no matching entries could be found.

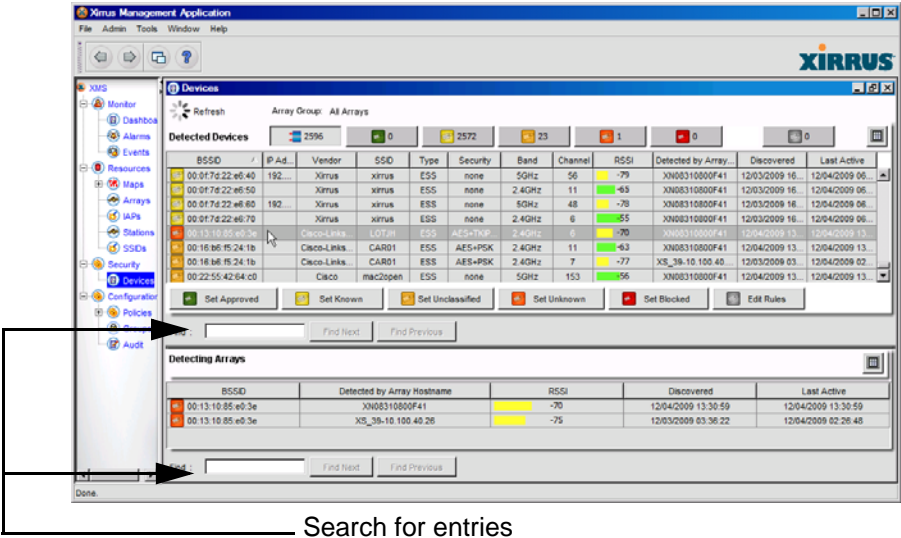


Figure 44. Searching for an Entry

XMS searches for the string in every column of the table, potentially matching many entries. For example, searching for an IP address by entering the string **200** will also find entries with a date in 2008 or 2009. Searching for **.200** instead is more likely to match only IP addresses.

Rearranging and Resizing Columns in a Table

For easier viewing of the table data, you can rearrange the columns by dragging the column header and moving it to the required place in the table. This is helpful if you want to view a column data in close proximity.

To resize a column header, simply drag the right-side edge of the column to expand or reduce the width of the column. This can be helpful when the data in the column is wide and extends beyond the column's current width.

Viewing Row Details


Table rows in the Events window contain summary data that can be expanded to reveal detailed information about the data in a row. To expand a row, simply double-click the row or right-click the row and choose **Details** from the pull-down list. Another option, for performing the same function (though more time-consuming) is to select a row then go to **View** in the **Menu Bar** and choose **Details**. (Figure 45)



Figure 45. Row Details (Expanded from a Row)

Searching for Events

The XMS client interface provides a powerful search engine that allows you to search your network's database for monitored events based on the criteria you define. This particular search feature is available for the Events and Audit windows only. To search tables in other windows, see [“Searching for Table Entries” on page 61](#).

To initiate a search from the Events window, go to **Edit** in the **Menu Bar** and choose **Search**, or click  in the tool bar at the top left.

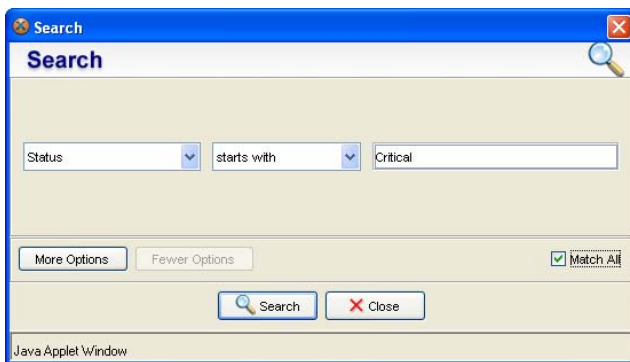


Figure 46. Using the Search Engine

Keyboard Shortcuts

Keyboard shortcuts are useful for experienced users who want to access, monitor or manage their network more quickly than a typical mouse allows. The following table shows the most commonly used keyboard shortcuts that are recognized by the XMS client interface. Be aware that some shortcuts are the same but invoke different commands depending on which window is the currently active window. It is assumed that only experienced users will take advantage of these keyboard shortcuts. Xirrus assumes no responsibility for misconfigured devices or networks caused by neglect or inexperience.

Action	Shortcut
Add new (map view only)	Ctrl+N
Broadcast a message	Ctrl+G
Close all windows	Ctrl+Shift+O
Close the currently active window	Ctrl+Shift+C
Deselect an object	Ctrl+Click
Detach window	Ctrl+Shift+T
Discover a network or an Array (Arrays, SSIDs, IAPs, or stations view only)	Ctrl+D
Discover a network or an Array (map view only)	Ctrl+C
Exit client interface	Alt+F4
Go back to the previous window	Ctrl+Shift+B
Go forward to the next window	Ctrl+Shift+F
Notifications setup (from alarm or event viewer)	Ctrl+Shift+A
Refresh the view	F5
Relayout a map	Ctrl+R

Action	Shortcut
Save a map layout	Ctrl+S
Search event (from the event viewer)	Ctrl+F
Select multiple entries in list or map	Ctrl+Click
Select a range of entries in list or map	Shift+Click
View About window	Ctrl+B
View help	F1
View row details in table (from the Events or Syslog window)	Alt+D

Discovering the Network

XMS can discover, authenticate and add Xirrus Wi-Fi Arrays and Power over Gigabit Ethernet (PoGE) injectors to its database. This discovery feature makes large scale Wi-Fi Array deployments quick and easy.

This chapter provides information about the discovery process, and includes procedures that describe how to add Xirrus devices manually (Arrays and PoGE injectors) and how to edit discovered networks and devices. In the rest of this chapter, the term *device* refers to a Xirrus Array or PoGE injector.

To quickly get discovery started on your Wi-Fi network, see the steps in **“Overview of Starting Discovery” on page 68**.

Section headings for this chapter include:

- **“Overview of Starting Discovery” on page 68**
- **“How Discovery Works” on page 70**
- **“Viewing Your Discovered Networks and Devices” on page 72**
- **“Scheduling Discovery” on page 74**
- **“Adding a Network” on page 78**
- **“Adding or Deleting Array Shell Authentication Entries” on page 80**
- **“Adding or Deleting SNMPv2 and SNMPv3 Entries” on page 81**
- **“Modifying a Network” on page 84**
- **“Rediscovering a Network” on page 85**
- **“Deleting a Network” on page 86**
- **“Adding an Array or PoGE Injector” on page 87**
- **“Refreshing a Device” on page 88**
- **“Deleting a Device” on page 89**
- **“What If My Device Is Not in the Discovered Devices List?” on page 89**

***NOTE:** For discovery of a device (Array or PoGE injector), the device must have SNMP enabled and its community string must match one of the strings listed in the Discovery*

window. See “**Adding or Deleting SNMPv2 and SNMPv3 Entries**” on page 81. The default SNMPv2 community string in XMS matches the Array default value.

NOTE: To use SNMPv3 successfully, system time must be set using an NTP server on both the XMS server host machine and all Arrays using SNMPv3. This is because SNMPv3 requires synchronization between the XMS server and the Arrays so that the system time difference between them never exceeds more than 150 seconds. If the time difference exceeds 150 seconds, SNMPv3 suspects a security breach and removes the SNMPv3 credentials for affected Arrays from the database. This means that the Array will appear to be down and statistics will not be polled until the Array is re-discovered by scheduled discovery (unless discovery is turned off). A manual refresh of the Array should also remedy the situation. See “**Scheduling Discovery**” on page 74 and “**Refreshing a Device**” on page 88.

Overview of Starting Discovery

This section provides a quick summary of the steps required to start the discovery process. For more details on any aspect of discovery, please see the other sections of this chapter, listed under **Discovering the Network**.

Once started, XMS Discovery uses SNMP to automatically find Xirrus Arrays and PoGE injectors in the subnets that you specify. (Figure 47) No networks are included in discovery by default, so you must add the subnets containing your Arrays.

1. Open an XMS Java client window and select **Discover Devices** from the **Tools** menu. The Discover Devices window shows networks, Arrays, and injectors that have been discovered and the status of discovery for each network. The devices that are shown are the only ones that are known to XMS and thus, they are the only ones that may be managed by it.
2. To add **SNMPv2 Community Names** or **SNMPv3 Users** to match the strings being used by your Arrays, click the appropriate **Add** button. For XMS to discover and manage a device, the device must have SNMP v2 and/or v3 enabled. The device’s SNMPv2 community string or SNMPv3 read-write authentication settings must match one of those defined here for discovery.

Discovery’s default SNMPv2 community name (**xirrus**) allows XMS to discover new Arrays that still have default SNMP settings (SNMPv2 is enabled with its **Read Write Community String** set to **xirrus**). Also, each Array’s **Trap Host 1 IP Address** is set to the hostname **Xirrus-XMS** by default (for the **Phone Home** feature).

- 3. To add networks for discovery, click the **Add** button under **Search Networks**. Enter the subnet’s **IP Address** and **Subnet** mask. Click **Apply**.

Discovery begins soon after adding a network. Be careful to specify the subnet accurately, to avoid creating excess traffic by discovering a needlessly large network.

To add individual Arrays or power supplies for discovery, click the **Add** button under **Discovered Devices**. Enter the device **IP Address** and click **Apply**.

Discover Devices
Discover Xirrus Devices Based on Networks and Community Names

Search Networks

IP Address	Subnet	Status
10.100.54.0	255.255.255.128	Discovery Complete
10.100.23.0	255.255.255.0	Discovery Complete
10.100.44.0	255.255.255.0	Discovery Complete

Array Shell Authentication

Username	Password

SNMPv2 Community Names

Community Name
xirrus
alibaba

SNMPv3 Users

Username	Authentication	Privacy
xirrus-rw	SHA	DES

Discovered Devices

Gig1 MAC	IP Address	Device Type	SNMP Version
00:0f:7d:00:12:16	10.100.54.19	Array	v2
00:0f:7d:00:49:aa	10.100.54.23	Array	v2
00:0f:7d:00:26:35	10.100.54.22	Array	v2
00:0f:7d:00:91:7a	10.100.54.26	Array	v2
00:0f:7d:00:4b:1c	10.100.54.27	Array	v2
00:0f:7d:01:35:0e	10.100.54.28	Array	v2
00:0f:7d:00:5e:f2	10.100.54.31	Array	v2
00:0f:7d:01:31:97	10.100.54.36	Array	v2
00:0f:7d:00:42:9b	10.100.54.37	Array	v2
00:0f:7d:00:46:4e	10.100.46.30	Array	v2
00:0f:7d:e0:00:0d	10.100.54.49	Pogetnjector	v2
00:0f:7d:00:9d:4f	10.100.54.50	Array	v2

56 devices

Auto Discover Schedule Close

Annotations:

- Networks
- Array Logins
- SNMPv2
- SNMPv3
- Arrays and Injectors

Figure 47. Managing Discovery of Devices

4. To manage auto-discovery scheduling, click **Auto Discover Schedule**.

By default, discovery runs daily at 23:00 hours.

*NOTE: When an Array boots up, it sends an SNMP trap to the XMS server's default hostname, **xirrus-xms**. XMS can then add it to its discovered devices list. This Phone Home feature requires DNS to resolve the hostname **xirrus-xms** correctly. Thus, if you change the host name of the XMS server, you must configure DNS to resolve **xirrus-xms** to the actual name of the XMS server host.*

How Discovery Works

XMS has two main ways of getting Arrays and managed PoGE injectors added to its database: the **Phone Home** feature that relies on an Array sending an SNMP trap to the XMS server's hostname, and the **Discovery** tool that uses SNMP.

Phone Home

Any time an Array boots up or its IP address changes, it announces its presence on the network. It does this by sending an SNMP trap to the XMS server's default hostname, **xirrus-xms** (this name is not case-sensitive). XMS can then communicate with the device, and add it to the **Arrays** window. The Phone Home feature requires DNS being properly configured in the network, so that the hostname **xirrus-xms** can be resolved to the IP address of the XMS server.

*NOTE: Arrays always send the SNMP trap to **xirrus-xms**. If you change the host name of the XMS server, you **must** configure your DNS server to redirect queries for **xirrus-xms** to the actual name of the XMS server host.*

As soon as a new device is plugged in, it "adds itself" to XMS without waiting for the next time discovery is run on the network. This reduces network overhead by greatly reducing the need for discovery and the traffic overhead that accompanies the process. Any devices that phone home to XMS are added to the appropriate list in the **Discover Devices Window** and become part of the XMS **Managed Network**.

Discovery

XMS's discovery feature uses SNMP to find networks and devices that are reachable from the server's network. Despite the advantages of the Phone Home

feature, discovery is still needed when you first start using XMS. Discovery will find your current network of Xirrus devices, without waiting for them to announce themselves as a result of being booted up. In some networks, discovery must be used because DNS is not configured to allow devices to resolve the hostname xirrus-xms.

***NOTE:** If you do not have a valid license for the XMS server, you are limited to managing one Array. Valid XMS licenses are typically for a particular number of Arrays. In either case, when XMS has discovered the maximum permitted number of Arrays, no additional Arrays will be discovered. See “**Licensing the XMS Server**” on page 35.*

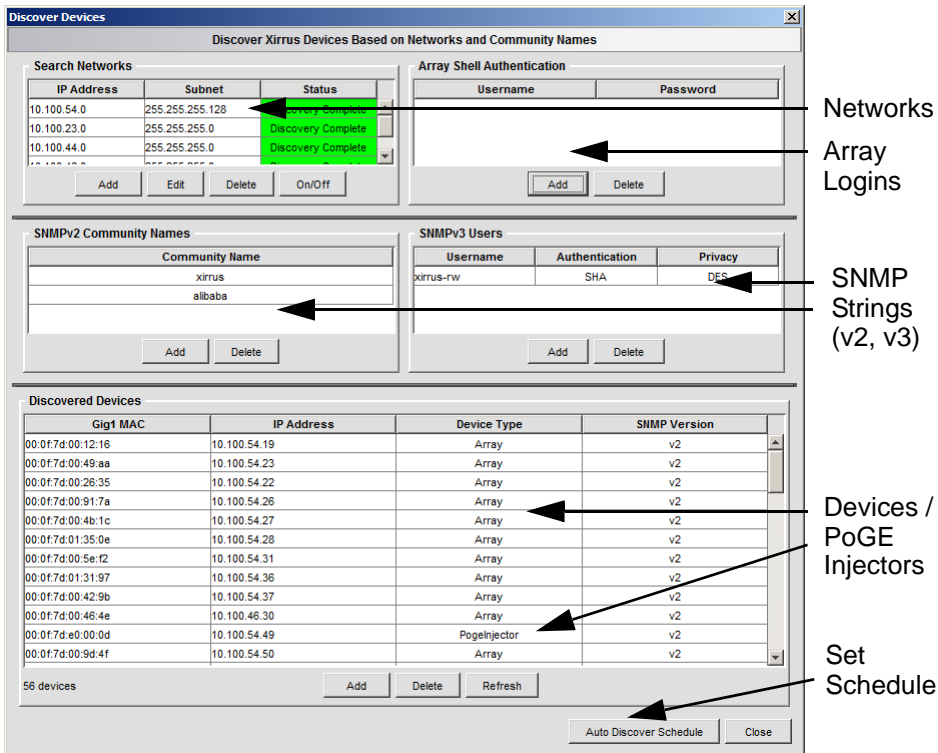
Any items (networks or devices) that are found by XMS are added to the appropriate list in the **Discover Devices Window** and become part of the XMS **Managed Network**. You have the option of initiating a rediscovery process on demand (for networks), or you can establish a schedule for the automatic discovery process in the **Scheduling Discovery** window. Scheduling is useful when the network is undergoing large-scale changes, such as the installation of a large number of Arrays. For a mature network, it is typically unnecessary to run discovery on a scheduled basis.

Devices that do not have SNMP enabled will **not** be discovered by XMS—in this case, go to “**Adding an Array or PoGE Injector**” on page 87.

Once a discovered network or device is included in the list of managed items, you can then modify (edit) or delete the item, as needed. Only devices that are included in the list of manageable items in the **Discover Devices Window** can be managed by XMS, and only these items can be added to the default **main map**—or any custom maps that you create.

Viewing Your Discovered Networks and Devices

After you start discovery, XMS finds networks and devices (Arrays and PoGE injectors) that are reachable, and discovered devices are then added to the system's database of manageable items. To view a listing of discovered networks and devices, select **Tools > Discover Devices** in the **Menu Bar** to display the Discover Devices window.



Discover Devices

Discover Xirrus Devices Based on Networks and Community Names

Search Networks

IP Address	Subnet	Status
10.100.54.0	255.255.255.128	Discovery Complete
10.100.23.0	255.255.255.0	Discovery Complete
10.100.44.0	255.255.255.0	Discovery Complete

Array Shell Authentication

Username	Password

SNMPv2 Community Names

Community Name
xirrus
alibaba

SNMPv3 Users

Username	Authentication	Privacy
xirrus-rw	SHA	DES

Discovered Devices

Gig1 MAC	IP Address	Device Type	SNMP Version
00:0f:7d:00:12:16	10.100.54.19	Array	v2
00:0f:7d:00:49:aa	10.100.54.23	Array	v2
00:0f:7d:00:28:35	10.100.54.22	Array	v2
00:0f:7d:00:91:7a	10.100.54.26	Array	v2
00:0f:7d:00:4b:1c	10.100.54.27	Array	v2
00:0f:7d:01:35:0e	10.100.54.28	Array	v2
00:0f:7d:00:5e:f2	10.100.54.31	Array	v2
00:0f:7d:01:31:97	10.100.54.36	Array	v2
00:0f:7d:00:42:9b	10.100.54.37	Array	v2
00:0f:7d:00:46:4e	10.100.46.30	Array	v2
00:0f:7d:e0:00:0d	10.100.54.49	PoGEinjector	v2
00:0f:7d:00:9d:4f	10.100.54.50	Array	v2

56 devices

Auto Discover Schedule

Figure 48. Discover Devices Window

NOTE: If you do not have a valid license for the XMS server, you are limited to managing one Array. Valid XMS licenses are typically for a particular number of Arrays. In either case, when XMS has discovered the maximum permitted number of Arrays, no additional Arrays will be discovered. See **"Licensing the XMS Server"** on page 35.

In addition to providing a list of discovered networks and devices, the Discover Devices window allows you to configure SNMPv2 and SNMPv3 values, enter Array authentication information that XMS can use to access Arrays, and shows the details of each network and device. For each device, the list shows its MAC address and IP address, the device type (Array or injector), and the SNMP version used to discover it. This same SNMP version will be used for all subsequent SNMP communication with the device. For network discovery, the Discover Devices window shows the status of discovery on the network. The status for network discovery may be any of the following:

- **Discovering...**
The discovery process is currently in progress. You must wait until the process has completed before taking any further action.
- **Discovery Complete**
The discovery process has been completed successfully.
- **Disabled**
The discovery process has been disabled for this network.

If XMS has not discovered a device that you expected to find in the Discovered Devices list, see [“What If My Device Is Not in the Discovered Devices List?”](#) on [page 89](#).

Scheduling Discovery

This option provides a tool for scheduling when XMS conducts a new discovery process, either hourly, daily, or monthly. When scheduling, keep in mind that the process may generate a significant amount of network traffic when discovering a large network. The impact is greatly reduced by minimizing the sizes of subnetworks being managed. Take care not to accidentally specify a Class A network. When configuring devices, or when manually adding a network for discovery (**“Adding a Network” on page 78**), be sure that the subnet mask specifies only the subnetwork to be managed with XMS. You may also exclude selected networks by explicitly disabling discovery on them (**“Excluding a Network from Discovery” on page 84**).

While scheduling automatic discovery to run less often will reduce its impact on network traffic, there is a trade-off. Since configuration information is obtained only when a device is discovered, a longer discovery period may also tend to leave XMS with information that is not up-to-date.

To access the **Network Discovery Schedule** window, click on the **Auto Discover Schedule** button on the bottom of the Discover Devices window.

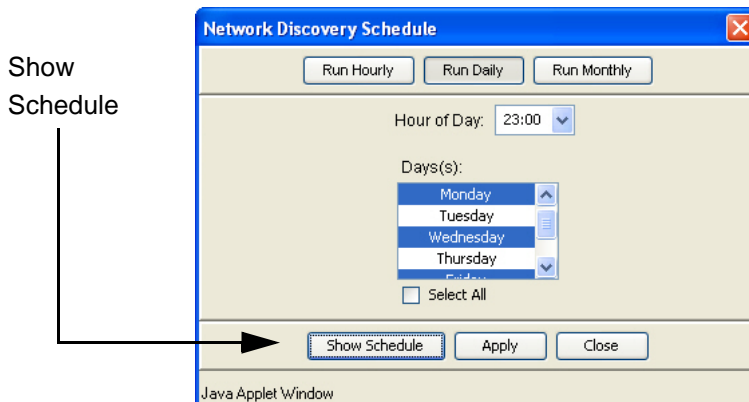


Figure 49. Network Discovery Schedule

Figure 49 shows an example of the Network Discovery Schedule window with the schedule set to **Run Daily** (Monday, Wednesday, and Friday at 23:00 in this

case). The editable fields in this window are dependent on which scheduling option you choose, either Hourly, Daily, or Monthly. The factory default is Daily at 23:00 hours (11 PM).

Some fields in the window may allow you to select more than one item from a list. For instance, in [Figure 49](#) you may select multiple days. Use **Ctrl+Click** to select additional items, or **Shift+Click** to select a range of entries. To select all entries (for instance, every day in this example), check the **Select All** check box. To clear all items (i.e., no items selected), click the **Select All** check box again. Click **Apply** when done.

Viewing the Discovery Schedule

To see the current discovery schedule for XMS, click **Show Schedule** in the [Network Discovery Schedule](#) window.

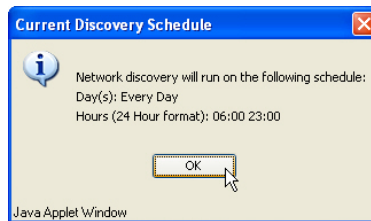


Figure 50. Viewing the Discovery Schedule

Scheduling Hourly Discovery

If you choose **Run Hourly**, the only editable field is the **Hours** field. In this case, select one or more hours from the list. Click **Apply**. The discovery process will start on the hour(s) that you specify every day of the week.

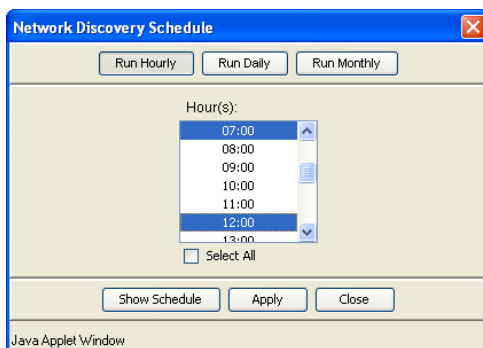


Figure 51. Scheduling the Discovery Process (Hourly)

Scheduling Daily Discovery

If you choose **Run Daily**, the only editable fields are the **Hour of Day** and **Days** fields. In this case, select an hour from the pull-down list, then select one or more days of the week—or click **Select All** if you want the discovery process to be initiated every day. Click **Apply**. The discovery process will start on the hour and day(s) of the week specified.

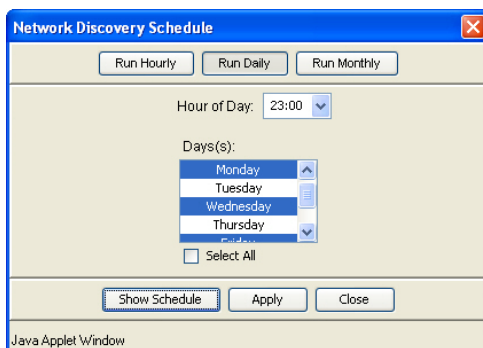


Figure 52. Scheduling the Discovery Process (Daily)

Scheduling Monthly Discovery

If you choose **Monthly**, the only editable fields are the **Hour of Day** and **Days** fields. In this case, select an hour from the pull-down list, then select one or more days of the month—or click **Select All** if you want the discovery process to be initiated every day. Click **Apply**. The discovery process will start on the hour and day(s) of the month specified. Note that discovery only runs on the selected days. If you select 30, then discovery will not run in February, for example.

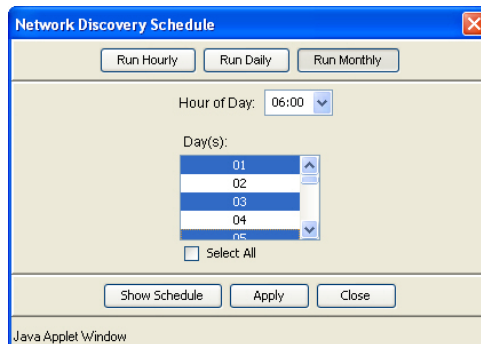


Figure 53. Scheduling the Discovery Process (Monthly)

When you have finished setting up the scheduling criteria for the network and device discovery process, click on the **Close** button to exit from the **Network Discovery Schedule** window.

Adding a Network

In addition to discovering networks, XMS allows you to add networks manually. To add a network, you must define its IP address and subnet. Discovery of a large network may generate a significant amount of network traffic, so be sure that the subnet mask specifies only the subnetwork to be managed with XMS, in order to minimize the impact of discovery on network traffic. Take care not to accidentally specify a Class A network.

To add a new network to the list of manageable networks, click on the **Add Network** button in the **Discover Devices Window** to display the Add Network window.

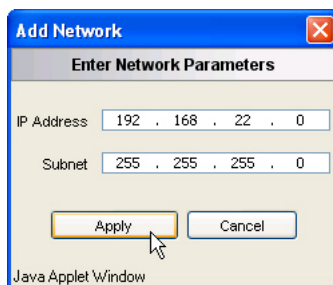


Figure 54. Adding a Network

Define the new network's IP address and subnet mask, then click the **Apply** button. After a few seconds the system generates a message informing you that the discovery process has started. Click on the **OK** button to close this window and return to the **Discover Devices Window**.

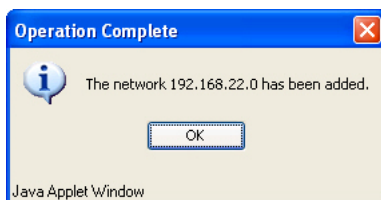


Figure 55. Network Added

In the **Discover Devices Window** you will notice that the **Status** column for the network indicates that discovery is still in progress.

In order for a device to be discovered, its SNMPv3 username/password or SNMPv2 community string must match one of those defined for discovery. See **“Adding or Deleting SNMPv2 and SNMPv3 Entries” on page 81** to verify that discovery’s search includes your community name.

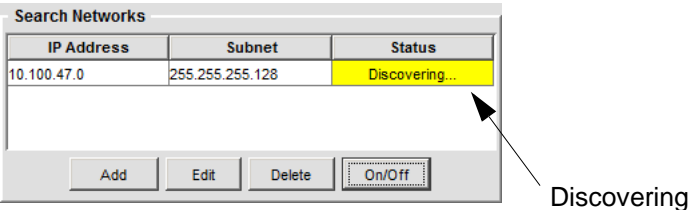


Figure 56. Network Discovery in Progress

When the network discovery process has finished, and if XMS is able to detect the network you are requesting, the status column in the **Discover Devices Window** changes from **Discovering** to **Discovery Complete**. This informs you that the system recognized the network you requested and the network can now be managed from XMS.

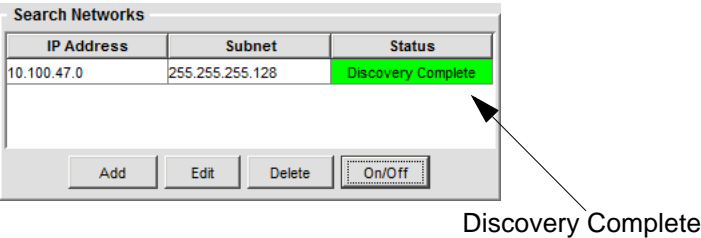


Figure 57. Network Discovery Finished

You may select an entry and use the **Edit** button to modify it, or use the **Delete** button to remove it. Use the **On/Off** button to disable discovery on the selected network. Click again to re-enable discovery.

Adding or Deleting Array Shell Authentication Entries

Some policies, such as **Software Update**, **Web Page Redirect (WPR)**, and **Configuration File (Advanced)**, require Arrays to download files. When it instructs an Array to fetch a file from the server, XMS must log in to the Array shell. Depending on the configuration of the Array, authentication may use the Array's local accounts or may use a RADIUS server. In either case, the XMS server needs to know a **Username** and **Password** to gain access to the Array shell.

To define Array login information, use the Array Shell Authentication section on the upper left of the Discover Devices window.

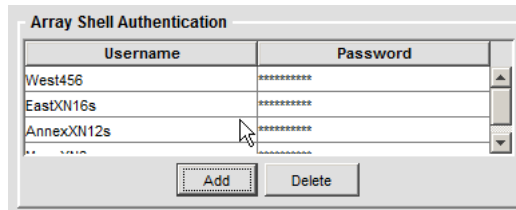


Figure 58. Array Shell Authentication

To create a new login, click the **Add** button. The Add Authentication dialog appears.

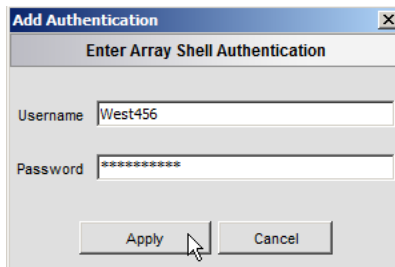


Figure 59. Adding an Array Shell Login

Enter an Array's **Username** and **Password**, and click **Apply**. The new entry will appear in the Array Shell Authentication list. You may use the **Delete** button to remove a selected entry, if necessary.

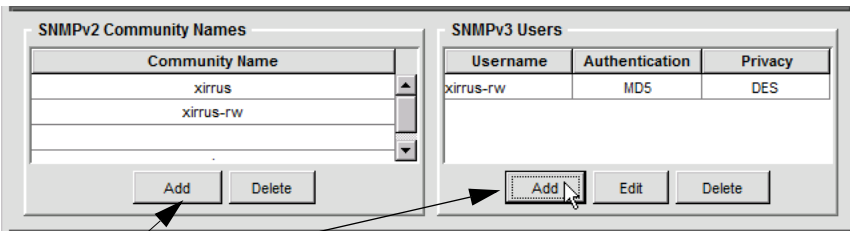
These authentication entries are not used by the discovery process itself, but are managed on this window for convenience. When XMS needs to log in to an Array's shell, it tries entries from the list until it finds one that works. Then it will remember to use this login for this Array. On future login attempts to the same Array, it will try the remembered login first.

Adding or Deleting SNMPv2 and SNMPv3 Entries

NOTE: For a device to successfully **Phone Home** (announce its presence to XMS) or be discovered, SNMPv2 or SNMPv3 must be enabled on the device. For SNMPv2, the read-write community string (i.e., community name) must match one of the strings listed in the Discovery window. For SNMPv3, the Array's read-write user name and passwords must match one of the entries listed in the Discovery window.

The XMS discovery process searches networks using both SNMPv2 and SNMPv3. Since SNMPv3 offers much improved security, this version is preferred by XMS. Discovery will search for devices using SNMPv3 first. When an Array is discovered using SNMPv3, then XMS uses that version for communication with the Array from then on. When an Array or PoGE injector is discovered via SNMPv2, then XMS uses SNMPv2 to communicate with the device. Injectors support SNMPv2 only.

SNMP v2 and v3 settings are shown in the SNMP section of the **Discover Devices Window**.



Community Name
xirrus
xirrus-rw

Username	Authentication	Privacy
xirrus-rw	MD5	DES

Add

Figure 60. SNMP v2 and SNMP v3 Configuration

XMS discovery has default SNMPv2 entries which match the factory default SNMP v2 settings in Arrays and PoGE injectors. However, for proper security on

your Xirrus devices, we **STRONGLY** recommend that you change these defaults on Xirrus devices by entering your own SNMPv3 user names and passwords and/or SNMPv2 community strings. Thus, you must add those community names or user names/passwords to XMS for discovery to find those devices.

***NOTE:** Although XMS does not have any SNMPv3 usernames or passwords defined by default, Xirrus Arrays do have default entries. The Array's default read-write username and password are **xirrus-rw**; the default read-only username and password are **xirrus-ro**.*

To add an **SNMPv3 User**, click the **Add** button under the right-hand list as shown above. The Add User dialog box appears.


The image shows a Windows-style dialog box titled "Add User" with a close button (X) in the top right corner. Below the title bar is a section header "Enter SNMPv3 User". The dialog contains five input fields: "Username" with the text "myUsername", "Authentication Password" with masked characters "*****", "Privacy Password" with masked characters "*****", "Authentication" with a dropdown menu showing "SHA", and "Privacy" with a dropdown menu showing "DES". At the bottom of the dialog are two buttons: "Apply" and "Cancel".

Figure 61. Adding an SNMPv3 Username

Enter the new **Username** and **Authentication** and **Privacy Passwords**. Set the **Authentication** and **Privacy** settings to match your Arrays. Click **Apply**.

To add an **SNMPv2 Community Name**, click the **Add** button under that list as shown (**Figure 60**). The Add Community dialog box appears. Enter the new name and click **Apply**.

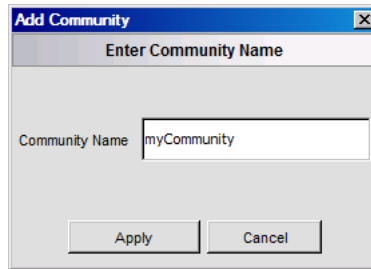


Figure 62. Adding an SNMPv2 Community Name

The next time that the discovery process runs after adding a new SNMP v2 or v3 entry, XMS will use all of the Community Names or Users listed. Adding or deleting a name on a list will not trigger discovery to run immediately. The new name will be used by the next discovery process (but will not be used now, if discovery is currently running). To trigger a discovery process using the new entry, see **“Rediscovering a Network” on page 85**.

To delete an entry from either list, select it and click **Delete**. You will be asked to confirm the deletion. The next time that the discovery process runs, it will use the Community and User Names listed at that time. Note that discovery will not remove devices from its device list if they have a community or user name that was deleted. Once a device is discovered, it stays on the device list even if you remove the community or user name or disable discovery. The device remains until you delete it manually.

You cannot modify an entry in the Community Names list, but you may delete it and then add the new value. You may click **Edit** to modify a selected SNMPv3 User entry. The next time that the discovery process runs, it will use the new value. Note that discovery will not remove devices from its device list if they have a community or user name that was changed. XMS will continue to manage the device using the original community or user name as long as the device is still configured to use them. If the device community or user name is changed, XMS will try to use the new values in the next discovery process.

Modifying a Network

You may want to change the properties of an existing network. To modify the discovery properties of a network, select a network from the list of available networks then click on the **Edit** button under the Search Networks list in the **Discover Devices Window** to display the Edit Network Parameters window. Make any necessary changes to the network's IP address, subnet mask and community setting, then click on the **Save** button to save your changes.

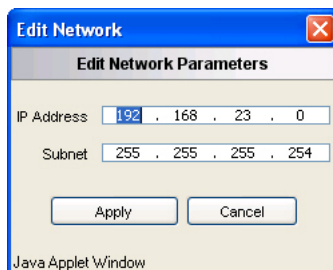
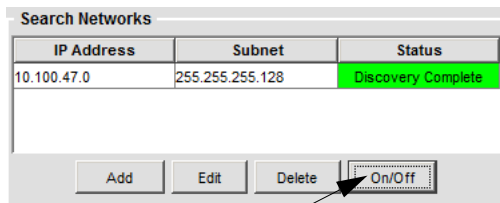


Figure 63. Modifying an Existing Network

Excluding a Network from Discovery

Since discovery can impact network performance, it's advisable to limit discovery to Class C networks where possible.



Enable/Disable

Figure 64. Disabling Discovery on a Network

To prevent discovery from running on a network in the Search Networks list, select the network and click the **On/Off** button. Note that discovery will not remove devices from its list if they are on a network where discovery has been disabled. Devices remain on the list until you delete them manually.

Rediscovering a Network

If you need to rediscover (refresh) an existing network, simply disable and then re-enable the network as follows. Select a network from the list of available networks, and click on the **On/Off** button in the Search Networks section to disable discovery on that network. Then click the button again to enable discovery. Whenever the a network transitions to enabled, discovery is triggered.

During the rediscovery process, the status column in the **Discover Devices Window** indicates that network discovery for the selected network is in progress. When the network has been successfully rediscovered (refreshed) by the system the status column indicates that the process is complete. **Figure 57 on page 79** shows an example of the Discovery window after completion.

Deleting a Network

If you need to delete an existing network from the Search Networks list, select the network you want to delete, then click on the **Delete** button underneath the list. A pop-up confirmation message is displayed requesting you to confirm that you want to delete the selected network.

Note that discovery will not remove that network's devices from its device list if the network is deleted. The devices remain until you delete them manually.

In the pop-up confirmation message, click on the **Yes** button to delete the selected network, or click on the **No** button to abort the request. The deleted network will be removed from the list of networks for discovery.

Select the Network

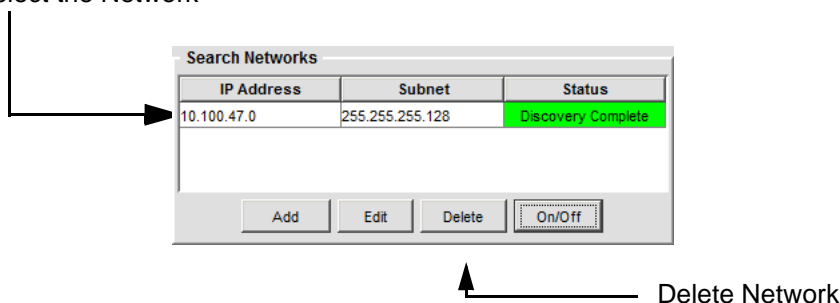


Figure 65. Deleting a Network

Adding an Array or PoGE Injector

Before you can add an Array or injector to the XMS list of manageable devices, the device must have SNMP enabled and its username/password or community string must match one of the community names configured for discovery (see [“Adding or Deleting SNMPv2 and SNMPv3 Entries” on page 81](#)). Unless SNMP is enabled on a device, XMS cannot identify it. To enable SNMP on a device and check its username/password or community string, refer to the *Wi-Fi Array User’s Guide*, part number 800-0006-001 or the *Power over Gigabit Ethernet Installation and User Guide*, part number 812-0057-001.

In addition to discovering Xirrus devices, XMS allows you to add devices manually, simply by entering the device IP address. To add a new device to the list of manageable devices, click on the **Add** button under the Discovered Devices list in the **Discover Devices Window** to display the Add device dialog box.

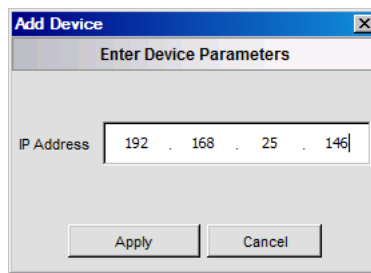


Figure 66. Adding a Device

Enter the new device’s IP address and click on the **Apply** button.

XMS will attempt to contact the device using SNMPv3, and if that is unsuccessful, it will try using SNMPv2. If the device is detected by XMS it is added to the list, along with the SNMP version that succeeded. Otherwise a pop-up message is displayed informing you that the device cannot be detected. In this case, click **OK** to close the message, then check the IP address that you entered for the device. For additional troubleshooting suggestions, see [“What If My Device Is Not in the Discovered Devices List?” on page 89](#).

Refreshing a Device

When you refresh a device, XMS polls the device and verifies that it is still reachable by the system. If you need to refresh an existing device, select it from the list of Discovered Devices then click on the **Refresh** button under the list in the **Discover Devices Window**.

The refresh process for a selected device may take a few seconds to complete, depending on the connection speed, so be patient while the process is being performed. A pop-up message is displayed when the refresh process has completed successfully. Click on the **OK** button to close the message window and return to the **Discover Devices Window**.

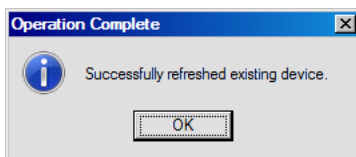


Figure 67. Refreshing a Device

If the refresh process fails, this is because XMS could not establish a connection with the selected device. In this case, check the network connectivity of the device. If the device has connectivity, see **“Why will XMS not discover an Array, even though the Array is connected to the network and functioning correctly?”** on page 542.

Deleting a Device

If you need to delete an existing device from the discovered list, select the device you want to delete then click on the **Delete** button under the Discovered Devices list in the **Discover Devices Window**. A pop-up confirmation message is displayed requesting you to confirm that you want to delete the selected device. The deletion cannot be undone—XMS will need to rediscover the device before it can be restored (see **“Adding an Array or PoGE Injector” on page 87**).

In the pop-up confirmation message, click on the **Yes** button to delete the selected device, or click on the **No** button to abort the request. The deleted device will be removed from the list of manageable devices. Note that a deleted device will be re-added to the list if it is found the next time that discovery runs, as long as XMS is still able to communicate with it via SNMP. You cannot tell the discovery process to ignore specific device(s) on the network.

What If My Device Is Not in the Discovered Devices List?

*NOTE: If you do not have a valid license for the XMS server, you are limited to managing one Array. Valid XMS licenses are typically for a particular number of Arrays. In either case, when XMS has discovered the maximum permitted number of Arrays, no additional Arrays will be discovered. See **“Licensing the XMS Server” on page 35**.*

XMS Discovery will find devices that are reachable from the XMS server’s network if their SNMP settings match those configured on the XMS server. If your Array or PoGE injector has not been discovered, check the following.

1. Have you discovered the maximum number of Arrays allowed by your XMS license?
2. Is the device powered up and fully booted?
3. For an Array—is SNMP enabled? (SNMPv2 is always enabled on Xirrus managed PoGE injector models.)
4. Does the XMS server have connectivity to the device (i.e., is the device connected and can you ping it?).
5. In the **SNMPv2 Community Names** and **SNMPv3 Users** sections, verify that one of the listed entries matches the SNMP values configured on the

device. If not, click **Add** under the appropriate list if you need to create a new entry. It is *crucial* that the values used by the device and by XMS match.

6. In the Search Networks section, verify that the subnetwork containing the device is listed, and that it is enabled. If not, click **Add** to enter it. After a few seconds the system generates a message informing you that discovery has started on the newly added network.
7. Discovery normally runs at scheduled times. To launch discovery immediately on a network, see [“Rediscovering a Network” on page 85](#).
8. You may add a device to the Discovered Devices section explicitly, using its IP address. Click **Add** at the bottom of the section, and enter the IP address. If the device is detected by XMS it is added to the list, otherwise an error message is displayed. In this case, check the IP address that you entered.

Using the Dashboard

The XMS Dashboard in the Java client gives you an at-a-glance overview of all system status and activity. Administrators can quickly assess system health and overall system performance, as well as viewing security status.

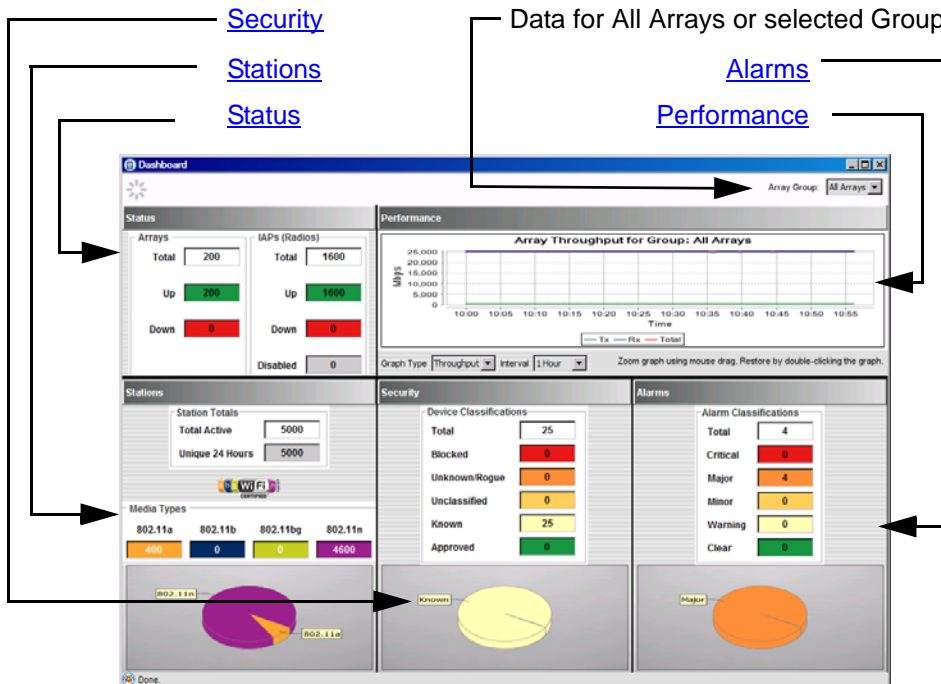


Figure 68. Dashboard

The following sections describe the use of the Java client Dashboard:

- [“Dashboard Overview” on page 92](#)
- [“Status” on page 94](#)
- [“Stations” on page 96](#)
- [“Performance” on page 98](#)
- [“Security” on page 100](#)

- “Alarms” on page 102

Dashboard Overview

When you start the XMS Java client, the main window opens with the Dashboard displayed. To navigate to it when you have another window displayed, open the Monitor node on the tree and select **Dashboard**.



The Dashboard behaves like any other window in XMS with respect to resizing, moving, detaching, closing, etc. The most convenient way to use the Dashboard is to open it into a separate window using the Detach button on the main toolbar. This allows you to keep it available on your desktop at all times, even when you’re working with other XMS windows (or other applications). (See “Basic Window Operations” on page 53).

You may resize the relative height of the top and bottom sections of the Dashboard. Simply click and drag a horizontal border between sections to change the sizes of sections.

About Dashboard Data

The Dashboard displays data for all Arrays in the XMS **Managed Network** by default. You may display data for just a selected group of Arrays using the **Array Group** field in the upper right corner (**Figure 68**). All sections of the Dashboard are updated to contain only data related to the selected Arrays (except for Alarms, which always shows all alarms). Other windows, such as **The Arrays Window** and **The IAPs Window**, will also display only data related to the selected group. These windows will name the group for which data is displayed. For example, the two windows just mentioned will show the selected group in the title of the Throughput chart. Select **All Arrays** on the Dashboard to return to showing data for the entire managed network.

The Dashboard is automatically refreshed at frequent intervals—you do not have to refresh explicitly. Note that some values displayed in the Dashboard may lag with respect to actual current values—items in the XMS database are polled (updated) at differing intervals. When the Dashboard is refreshed, it simply picks up the current values in the database. The XMS server does not poll all status or

statistics in the database specifically for a Dashboard refresh. Each data item in the database will be refreshed at whatever rate is defined for it. For more details on the polling rate and how to change it, please see [“Web Client — Polling Settings” on page 516](#) or [“XSMT - Advanced Settings” on page 537](#).

The Dashboard refreshes data at the following rates by default:

- **Performance** data is updated on the Dashboard every 30 seconds. (This is true for Arrays running Release 3.1 and higher software images.)
- Data for all other sections of the Dashboard is updated at least every two minutes.
- Alarms occur in real time. Traps generated by Arrays and other events with a severity greater than informational are displayed as alarms.

These rates may be modified using the [Xirrus Server Management Tool \(for Windows-based Servers\)](#). See [“Changing Polling Frequency” on page 537](#).

Status

The Status section summarizes the number of Arrays (up or down) for the selected **Array Group** (see [“About Dashboard Data” on page 92](#)), and summarizes the status of their IAPs as well.

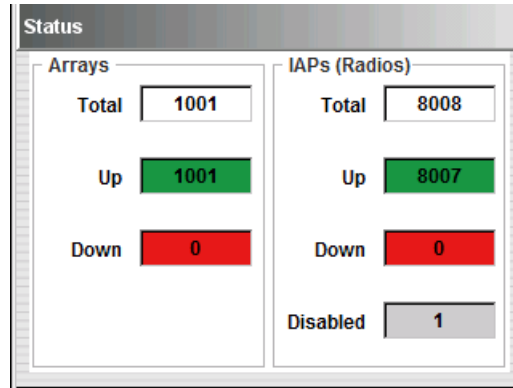


Figure 69. Dashboard - Status

Section Details

- **Arrays**

This is a summary of the status of the selected Arrays that are known to XMS.

The entries show the count of Arrays at each status value. Each entry is a link—click it to display [The Arrays Window](#), with the Array list filtered to show only those Arrays that have the selected status value.

The following status counts are shown:

- **White**—the **total** number of Arrays in the group. Click this button to show the selected Arrays in [The Arrays Window](#), regardless of status.
- **Green**—the number of Arrays that are **up**, in the selected group. Click this button to show only Arrays whose status is up in the Arrays window.

- **Red**—the number of Arrays that are **down**, in the selected group. An Array is considered to be down if XMS has been unable to communicate with it for over three minutes. Click this button to show only Arrays that are down in the Arrays window.

- **IAPs**

This is a summary of the status of all IAPs on Arrays that are in the selected group.

The entries show the count of IAPs at each status value. Each entry is a link—click it to display **The IAPs Window**, with the IAP list filtered to show only those IAPs that have the selected status value.

The following status counts are shown:

- **White**—the **total** number of IAPs in the group. Click this button to show all IAPs in the IAPs window, regardless of status.
- **Green**—the number of IAPs that are **up**. Click this button to show only IAPs whose status is up in the IAPs window.
- **Light Gray**—the number of IAPs that are not enabled on Arrays. Click this button to show only IAPs that are disabled in the IAPs window.
- **Red**—the number of IAPs that are **down**. Click this button to show only IAPs that are down in the IAPs window.

Stations

The Stations section summarizes the number of active stations for the selected **Array Group** (see “[About Dashboard Data](#)” on page 92), the proportion using 802.11a, 802.11bg, 802.11b, or 802.11n, and identifies the five stations with the poorest signal strength.

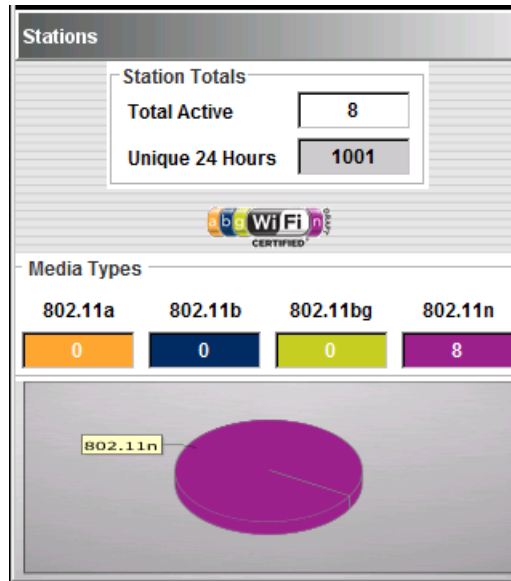


Figure 70. Dashboard - Stations

Section Details

- **Station Totals**

This shows the number of stations in the selected group. Click on a count to show [The Stations Window](#), with the station list filtered to show the selected stations.

- **Total Active**— the total number of stations currently associated to all selected Arrays.
- **Unique 24 hours**—the total count of unique stations (by MAC address) which associated across the selected Arrays over the last 24 hours. In other words, this is the count of all stations that have

associated to Arrays in the selected group in the last 24 hours, with no station counted more than once.

- **Media Types**

This is a breakdown of the number of 802.11a, 802.11bg, 802.11b, and 802.11n stations that are currently associated to the selected Arrays. The count of each station type is shown, and a pie chart illustrates the proportion of each type. Click on a count or a pie chart segment to show **The Stations Window**, with the station list filtered to show the selected stations.

Performance

This section summarizes recent performance or station associations for the selected **Array Group** (see **“About Dashboard Data” on page 92**) over the selected interval. You may select the **Graph Type: Throughput** or **Media Type**. The graph is automatically refreshed every 20 seconds.

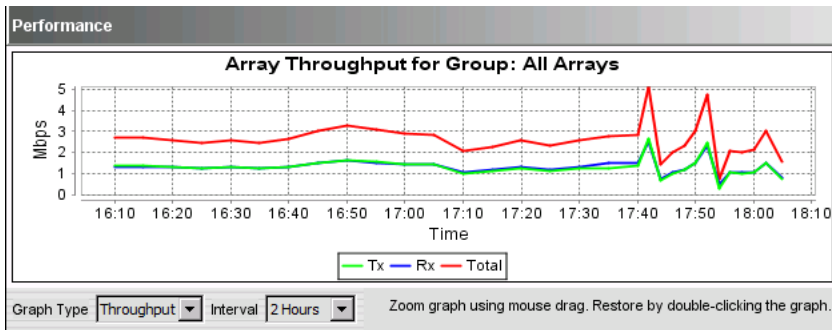


Figure 71. Dashboard - Throughput

Use the **Interval** drop-down list to select the time period to be graphed. The chart shows data for the last hour by default. If you change the **Interval**, a graph for that period of time will be displayed, up to approximately the current time. If you change the interval, XMS resource charts such as those on the **The Arrays Window** and **The IAPs Window** will automatically show the same time interval.

You may zoom in on an area of the graph by selecting the area of interest with the mouse. Click and drag to select a region. When you release the mouse button, the chart will show the selected region. Double-click anywhere in the chart to revert to showing the entire chart.

Section Details

- **Throughput**

The line graphs in this chart display aggregate data throughput across the selected Arrays.

This chart is very similar to the **Array Throughput** chart in **The Arrays Window**. Transmit throughput is shown in green, receive throughput is shown in blue, and total throughput is shown in red.

- **Media types**

The line graphs in this chart display the number of stations associated to the selected Arrays over time. The stations are broken down by media type, and the total number of stations is also graphed is also shown.

Security

This section provides a quick snapshot of the security status of the selected **Array Group** (see [“About Dashboard Data” on page 92](#)), including counts of known and rogue APs.

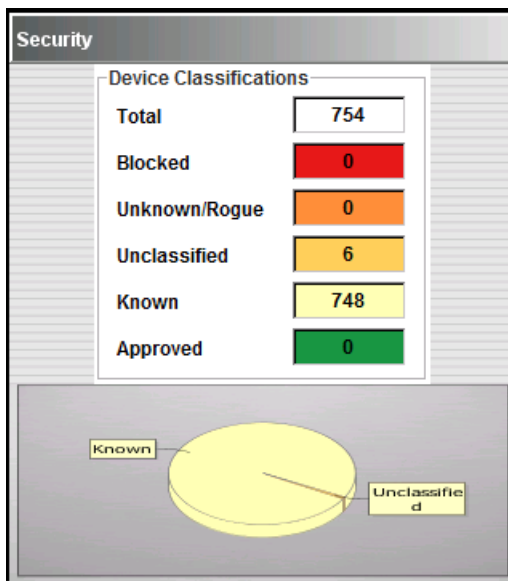


Figure 72. Dashboard - Security

For more information about security and intrusion detection, please see [“Security - Managing Intrusions” on page 119](#).

Section Details

- **Device Classifications**

This is a summary of the status of all APs that have been detected by the selected Arrays.

The total count of devices detected is shown, along with the total in each class, represented by color—Blocked, Unknown, etc. Each entry is a link. Click it, and **The Devices Window** is displayed, with the **Detected Devices** list showing just that class of device.

The classes and their representative colors are:

- **White—Total:** This is the sum of the number of detected devices of all classes. Each rogue is counted in this list exactly once—even if it was detected by multiple Arrays.
 - **Red—Blocked:** These are rogues that you have designated as blocked. An Array can block a rogue AP by taking measures to prevent stations from staying associated to the rogue.
 - **Orange—Unknown/Rogue:** These are rogues that you have designated as unknown.
 - **Gold—Unclassified:** When a device is initially detected, it is unclassified, which simply means that no one has classified it yet.
 - **Yellow—Known:** When a rogue is designated as Known the system stops reporting on it. It is no longer displayed in the **Rogue List** report.
 - **Green—Approved:** When a rogue is designated as Approved the system stops reporting on it. It is no longer displayed in the **Rogue List** report.
- **Pie Chart**

The pie chart is a graphical representation of the data in the **Device Classifications** section. The different classes of devices are represented by the same colors defined above. Hover the mouse over a segment and a tooltip appears to show the class that the segment represents. Each segment of the pie chart is a link. Click it, and **The Devices Window** is displayed, with the **Detected Devices** list showing just that class of device.

Alarms

This table displays a summary of the alarms displayed by the XMS Alarms window (see “Alarms” on page 107). All alarms are shown, even if you have selected an **Array Group**. All alarm levels are displayed—Critical, Major, Minor, Warning, and Clear.

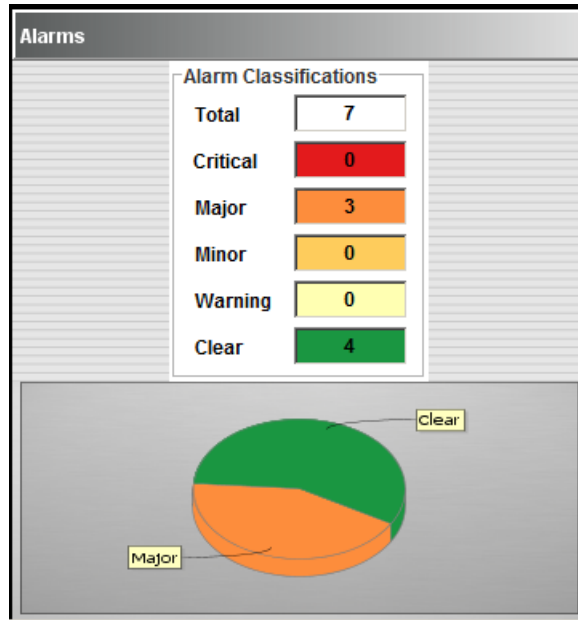


Figure 73. Dashboard - Alarms

Section Details

- **Alarm Classifications**

This list shows alarms that have been sent to XMS. The total count of alarms is shown, along with the total at each alarm level:

- **Critical**—Red
- **Major**—Orange
- **Minor**—Gold

- **Warning**—Yellow
- **Clear**—Green

Each entry is a link. Click it, and the **Alarms** window is displayed, showing only alarms at that level.

- **Pie Chart**

The pie chart is a graphical representation of the data in the **Alarm Classifications** section. The different alarm levels are represented by the same colors defined above. Hover the mouse over a segment and a tooltip appears to show the alarm level that the segment represents. Each segment of the pie chart is a link. Click one, and the **Alarms** window is displayed, showing only alarms at that level.

Monitoring Your Network

This chapter discusses the tools provided with the XMS Java client that allow you to monitor and manage any network events and alarms flagged by the system, with examples. Section headings for this chapter include:

- **[“At First Glance” on page 105](#)**
- **[“Alarms” on page 107](#)**
- **[“Events” on page 111](#)**
- **[“Syslog Events” on page 112](#)**
- **[“Email Notifications for Events and Alarms” on page 115](#)**

At First Glance

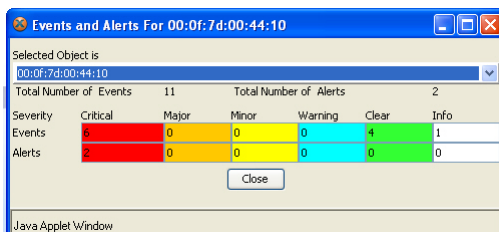
Any time you log in to the XMS Java client, the Dashboard provides an immediate, at-a-glance overview of the health and performance of your network. This should always be the first place that you look for an overview of network status. We recommend that you detach the Dashboard window, so that you can always have it visible on your display even while you’re working on other windows. For complete details on using the Dashboard, see **[“Using the Dashboard” on page 91](#)**.

The **Alarms**, **Events**, and **Syslog Events** windows provide summary and detailed information about the status of the XMS **Managed Network**. Other windows also provide a useful overview of network status. For example, resource windows provide visual cues to the status of network components in the **Arrays**, **IAPs**, and **Stations** windows.

Viewing Events and Alarms for a Specific Array

Before we discuss the details of syslog messages, network events and alarms, you need to be aware that you can view network events and alarms for a specific Array. This section only applies to events and alarms, because these are the only items that can be addressed by a specific Array. The syslog and topology categories apply to an entire network or subnet, not to Arrays.

To view all events and alarms that have been generated for a specific Array, right-click on the Array in a map or in the **The Arrays Window** to select it, then choose **Events and Alarms** from the pull-down list. All events and alarms for the selected Array are displayed in a pop-up window in tabular form, by severity level only. (Figure 74) This table includes an informational column that is color-coded as WHITE. Informational alarms (white) are not reported in the **Alarms** window.



Selected Object is 00:0f:7d:00:44:10						
Total Number of Events		11				
Total Number of Alerts		2				
Severity	Critical	Major	Minor	Warning	Clear	Info
Events	6	0	0	0	4	1
Alerts	2	0	0	0	0	0
<input type="button" value="Close"/>						
Java Applet Window						

Figure 74. Events and Alarms (By Array)

Alarms

Alarms are generated when the system detects a problem with the network that it determines must be resolved, and therefore alerts you to the issue. The Alarms window provides tools for reviewing and acting on an alarm. Only the current (most recent) alarm in each category for each device will be shown in this list.

SNMP traps and other **Syslog Events** (with a severity greater than informational) are treated as alarms, and thus are displayed in the Alarms window. SNMP traps range in severity from informational (for example, an administrator logging in) to critical (such as a failed software upgrade or an unreachable Array).

Syslog event severity is mapped to alarm severity as follows:

- Information, Notice, Debug -> Informational (no alarm)
- Warning, Alert, Error -> Warning Alarm
- Critical, Emergency -> Critical Alarm

The Alarms window is displayed when you click on the **Alarms** node in the **Tree**, which appears under the **Monitor** parent node. Information on this window is automatically refreshed every 20 seconds.

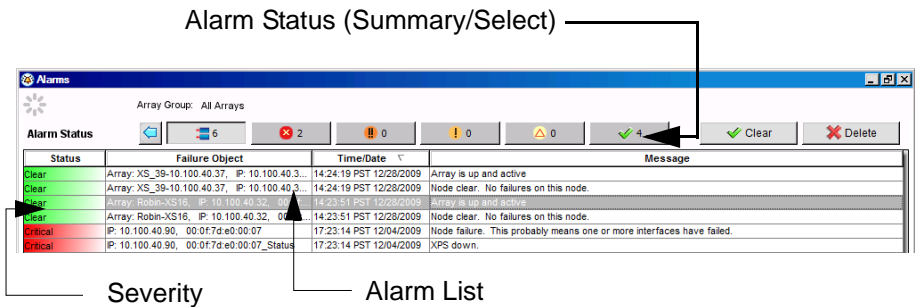



Figure 75. Alarms Window

The Alarms window is divided into two sections:

- **Alarm Status**—A count of alarms by severity: allows you to select the alarms to be listed.
- **Alarm List**—A list of alarms.

Alarm Status

The buttons at the top of the window summarize alarms by showing the count at each severity level. The buttons also allow you to select the alarms to be shown in the Alarm list based on severity. (Figure 76) Hover the mouse over a button to display the severity value represented by the button. You may display the **Dashboard** by clicking the blue arrow. 

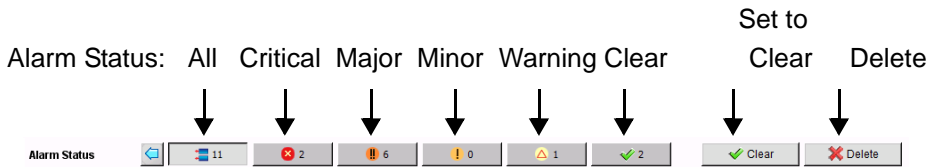


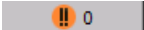
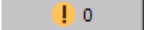

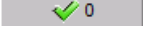


Figure 76. Alarm Status Summary/Select Buttons

The following severity buttons are shown. Click a button to filter the Alarm list, so that it shows only alarms with the selected severity. Please see **“Severity Levels” on page 110** for more information.

-  **Dark Blue—Total:** the **total** number of alarms in the network. Click this button to show all alarms in the Alarm list, regardless of severity.
-  **Red—Critical**
-  **Orange—Major**
-  **Gold—Minor**
-  **Yellow—Warning**
-  **Green—Clear**

The **Clear** and **Delete** buttons to the right of the severity buttons are used in conjunction with the Alarm list to clear alarms or delete them. You may select multiple alarms to clear or delete at once, using **Ctrl+Click**, **Ctrl+a**, or **Shift+Click**.

Alarm List

Status	Failure Object	Time/Date ▾	Message
Major	01:02:7d:00:4b:52_Trap	16:04:48 PDT 04/03/2008	Trap received softwareUploadFailure -
Minor	01:01:7d:00:4b:52_Trap	16:04:40 PDT 04/03/2008	Trap received resetArray -
Critical	01:00:7d:00:4b:52_Trap	16:04:36 PDT 04/03/2008	Trap received envCtrlTempOver -

Figure 77. Alarm List

This list shows alarms for the XMS **Managed Network**. Use the **Alarm Status** buttons to select which alarms to display—all alarms, or only those with the selected severity. For each alarm, the following information is shown:

- The **Status** is color-coded to denote the current severity of each alarm. See **“Severity Levels” on page 110**.
- The **Failure Object** shows the MAC address of the Array that sent the alarm. It may have a further indication of the source of the alarm appended to it, for example:
 - 00:0f:7d:03:6a:80_Status
 - 00:0f:7d:03:6a:80_Trap.
- The **Time and Date** that the alarm was received.
- The **Message** is a brief description of the condition that caused the alarm.

More detail on the Alarms window is discussed in the following topics:

- **Severity Levels**
- **Taking Action on an Alarm**

Severity Levels

The severity levels for all alarm categories are color coded, as follows:

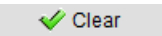
- **GREEN – Clear**
This state is reported when any problem that previously caused a critical (red) alarm has been resolved.
- **YELLOW – Warning**
This is letting you know that some action needs to be taken to avoid an alarm (an alarm has not yet been invoked, but probably will be if the warning is ignored).
- **GOLD – Minor**
A minor problem exists and should be investigated.
- **ORANGE – Major**
A major problem exists. If this problem is ignored there is a likelihood that the problem will escalate to a critical condition.
- **RED – Critical**
A critical failure has occurred within the network and the problem must be resolved immediately.

Taking Action on an Alarm

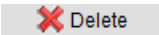
There are two ways to act on an alarm:

- **Clearing an Alarm**
- **Deleting an Alarm**

Clearing an Alarm

To set the severity of alarms to **clear**, select the desired entries in the Alarm list and click the **Clear** button.  Once an alarm is cleared, it will display as a cleared alarm and will no longer show its original severity.

Deleting an Alarm

To delete alarms from the Alarm list, select the desired entries in the Alarm list and click the **Delete** button. 

Events

This window displays network events detected by XMS. **Figure 78** shows an example of the Events window after selecting an event in the list to generate the Event details window.

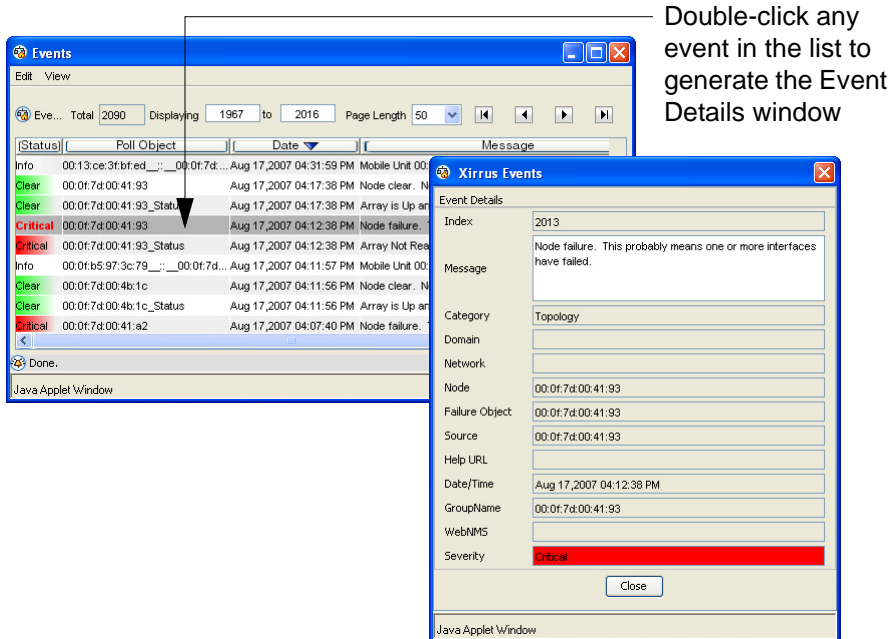


Figure 78. Reviewing Network Event Details

To generate the Event Details window and review the informational details behind any event, use any of the following procedures:

- Double-click on any event in the list.
- Right-click on any event in the list, then choose **Details** from the pull-down list.
- Click on any event in the list to select it (single click), then go to the Menu Bar and choose **View > Details**.
- Click on any event in the list to select it, then type **Alt+d**.

Review the details of the selected event in the Event Details window. When finished, click the **Close** button.

Syslog Events

Syslog is a protocol that allows a machine to send event notification messages across IP networks to event message collectors, known as syslog servers. Syslog messages are based on the [User Datagram Protocol \(UDP\)](#). They are received on UDP port 514 and cannot exceed 1,024 bytes in length (they have no minimum length).

XMS reconciles syslog activity on all Wi-Fi Arrays in the network. Syslog reporting is time-stamped, and to ensure that all syslog time-stamping is maintained by a universal clock for all Arrays, an NTP (Network Time Protocol) server should be enabled. Without an NTP server assigned (no universal clock), each Array will use its own internal clock and stamp syslog event times accordingly, which may result in discrepancies. For more information about using an NTP server, refer to the *Wi-Fi Array User's Guide*, part number 800-0006-001.

In addition to viewing syslog messages on the [Syslog Window](#), syslog events that trigger alarms occupy their place in the [Alarms](#) window. For more information about syslog events that trigger alarms, refer to [“Alarms” on page 107](#).

Configuring Syslog and NTP Servers

Syslog and NTP servers are configured when creating a [Services](#) policy. [\(Figure 79\)](#) The Services policy is then applied to your Arrays to configure them. As already mentioned, without an NTP server assigned all Arrays will use their own internal clock, which will cause time-stamping inconsistencies across syslog events. When configuring the syslog server, you have the option of specifying a maximum number of syslog messages retained internally and defining the reporting severity level. For more information about configuring a syslog and/or NTP server, go to [“Services” on page 247](#).

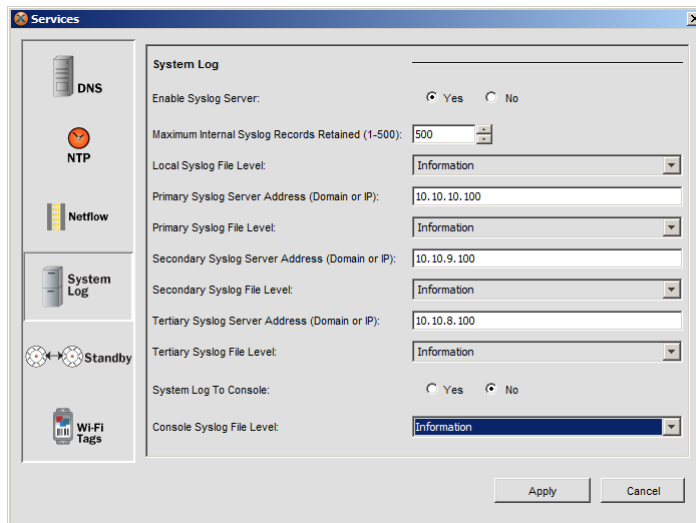


Figure 79. Configuring a Syslog Server

Syslog Severity Levels

All syslog messages are categorized by their levels of severity, which include:

- Emergency
- Alerts
- Critical
- Error
- Warning
- Notice
- Information (default)
- Debug (not to be used for routine syslog monitoring)

Reviewing Syslog Events

To review syslog events, click the **Tools** menu and select **Syslog** to open the Syslog window in your browser. All syslog entries are displayed initially, regardless of their severity level. Any event that has triggered an alarm is color-coded. To view the totals for all color-coded alarms, see the **Alarms** window.

Table is sorted by **Time** in descending order

Export filtered data

Browse to other pages

Select Columns Export

Showing 1 to 25 of 92245 Rows: 25 << 1 2 3 4 5 6 7 8 9

Time	Severity	Array IP Address	Mac Address	Array Hostname	Message
Oct 22, 2010 2:30 PM	Info	10.100.54.111	00:0f:7d:00:03:1f	XS0834081AA38	Oct 22 05:31:39: debug : Rogue AP blocked. SSID: pctest, BSS
Oct 22, 2010 2:30 PM	Info	10.100.54.29	00:0f:7d:01:95:b1	XN123810220A3	Oct 22 13:30:33: debug : Rogue AP blocked. SSID: pctest, BSS
Oct 22, 2010 2:30 PM	Info	10.100.54.28	00:0f:7d:01:35:0e	NORTA-Array5	Oct 22 13:26:27: debug : Rogue AP blocked. SSID: pctest, BSS
Oct 22, 2010 2:30 PM	Info	10.100.54.111	00:0f:7d:00:03:1f	XS0834081AA38	Oct 22 05:31:38: debug : Rogue AP blocked. SSID: pctest, BSS
Oct 22, 2010 2:30 PM	Info	10.100.54.111	00:0f:7d:00:03:1f	XS0834081AA38	Oct 22 05:31:38: debug : Rogue AP blocked. SSID: pctest, BSS

Figure 80. Syslog Window

You may use the search and filter capabilities to display only selected entries. (Figure 81) Select a **Severity** level from the drop-down list to display only syslog entries that are at that level.

Search string (full or partial)

Select Severity level

Date from: 10/20/2010 Time from: 00:00 Date to: 10/22/2010 Time to: 00:00

Search Text: upda Severity: All Severities Log Type: Syslog Search

Figure 81. Filtering Syslog Entries

To display only entries at the selected level that contain a particular string in the **Message** column or one of the other columns, enter it in the **Search** field and click **Search**. Case is ignored and partial strings are matched—thus searching for **ABGN** will match **abgn1** to **abgn4**. To return to displaying all syslog entries, clear the search field and set the severity level to **All Severities**, and click **Search**.

You may also specify dates as search criteria.

The events listed in the table can be sorted to best suit your viewing needs—the default is to have syslog events listed by Time (the first column), with the most recent entries on top. To change how the table is sorted, click in any column header to define that header as the sort criteria. Click the same header again to toggle between ascending and descending order.

If the Syslog table contains multiple pages of information, use the browse buttons provided in the top right corner of the window to navigate between pages. Use << or >> to jump to the first page or last page, respectively.

The **Export** button on the upper right may be used to export syslog entries to a CSV file—a set of comma-separated values that are compatible with Microsoft Excel. If you have applied a filter, then only the entries that satisfy the filter criteria will be exported. When you click **Export**, a dialog box will allow you to save the results in a file or open them in Excel.

Email Notifications for Events and Alarms

You can set up email notifications to be sent when specified network events or alarms occur. The email will identify the notifying Array by host name, IP address, and MAC address.

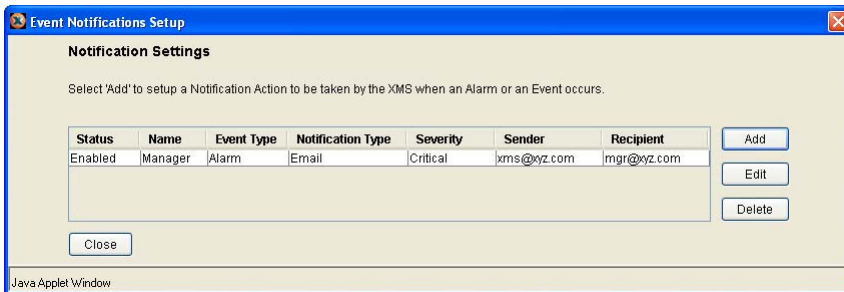
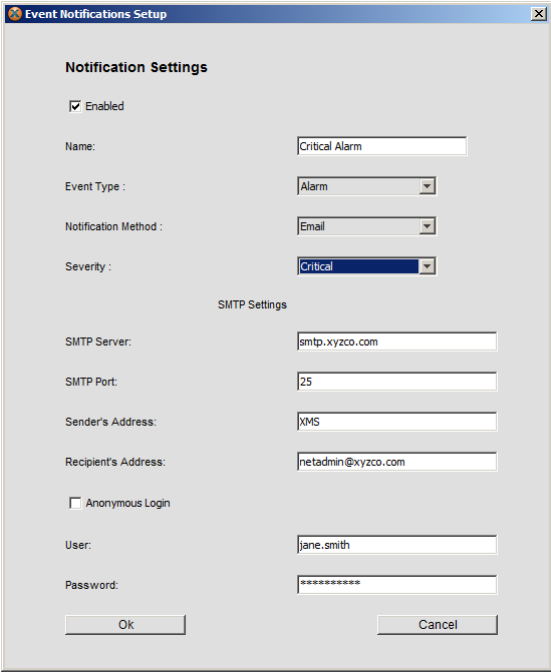


Figure 82. Event Notifications List

To set up an email notification, you must be in an alarms or events window. Click on the **Network Events** or **Alarms** node in the **Tree** to open the desired window. From the Edit menu, select **Notifications**, or simply enter **Ctrl+Shift+A**. **Figure 82** shows the Event Notifications List, which displays the notifications that you have already created. You may select an existing entry and modify or delete it using the **Edit** or **Delete** buttons. Note that you cannot change the order in which the entries are listed.

To create a new email notification, click the **Add** button. **Figure 83** shows the Event Notifications Setup window. Check the **Enabled** checkbox to enable this email notification to be sent when the selected condition occurs. You may clear the checkbox if you wish to disable the notification without deleting this entry. Enter a unique **Name** to identify this entry. Select the **Event Type** (Alarm or Event), and the **Severity**. An exact match of this severity level will trigger the sending of the notification. The only **Notification Method** offered is email.



The image shows a screenshot of the 'Event Notifications Setup' dialog box. It has a title bar with a close button. The main area is titled 'Notification Settings'. It contains several fields and checkboxes. The 'Enabled' checkbox is checked. The 'Name' field contains 'Critical Alarm'. The 'Event Type' dropdown is set to 'Alarm'. The 'Notification Method' dropdown is set to 'Email'. The 'Severity' dropdown is set to 'Critical'. Below these is a section titled 'SMTP Settings'. It contains fields for 'SMTP Server' (smtp.xyzco.com), 'SMTP Port' (25), 'Sender's Address' (XMS), and 'Recipient's Address' (netadmin@xyzco.com). There is an 'Anonymous Login' checkbox which is unchecked. Below that are fields for 'User' (jane.smith) and 'Password' (masked with asterisks). At the bottom are 'OK' and 'Cancel' buttons.

Notification Settings	
<input checked="" type="checkbox"/> Enabled	
Name:	Critical Alarm
Event Type :	Alarm
Notification Method :	Email
Severity :	Critical
SMTP Settings	
SMTP Server:	smtp.xyzco.com
SMTP Port:	25
Sender's Address:	XMS
Recipient's Address:	netadmin@xyzco.com
<input type="checkbox"/> Anonymous Login	
User:	jane.smith
Password:	*****
OK Cancel	

Figure 83. Event Notification Creation

To set up the mail recipient and server to be used, enter the following:

- **SMTP Settings: SMTP Server and Port**
In the **SMTP Server** field, enter the address of the mail server to be used for sending the notification, for example, **smtp.xyzco.com**. Enter the **SMTP Port** used by the server. The default value for the SMTP port is 25.
- **Sender and Recipient**
In the **Recipient's Address** field, enter the email address to which this notification should be sent. Enter an email address in the **Sender's Address** field - this will be used in the notification to identify the sender.
- **User and Password**
If the specified SMTP server allows anonymous users, then check the **Anonymous** checkbox and you will not need to enter a user name and

password. Otherwise, if the SMTP server requires users to log in, clear the **Anonymous** checkbox and then enter the **User** and **Password** for a valid SMTP account. Note that many IT administrators do not allow anonymous logins to their SMTP server, to thwart spammers. If you are not certain about how to access the SMTP server, check with your administrator.

Click **OK** when you are done, and the new notification is complete.

Security - Managing Intrusions

The Devices Window

To manage security in your wireless network, use the XMS **Devices** window. This window provides an overview of the security status of the network, including counts of known and rogue APs, the collective list of potential rogue devices detected by Arrays in the network, and types of encryption in use. The Arrays that detected the intruding APs are also identified.

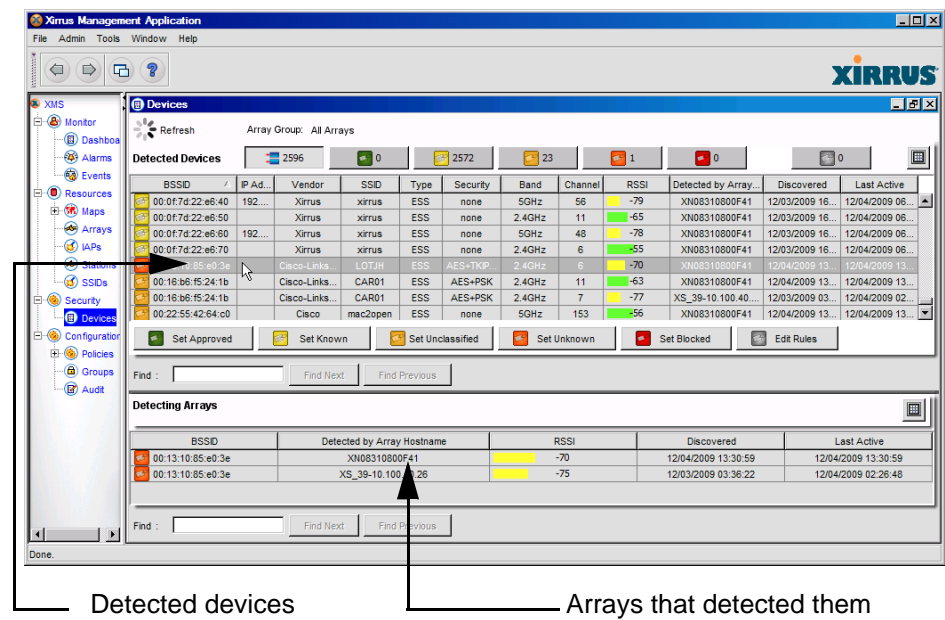


Figure 84. Security—Devices

To navigate to the **Devices** window, open the **Security** node on the tree and select **Devices**. You may also open this window from the **Security** section of the Dashboard—click the colored representation of any class of detected device and the Devices window will be displayed, showing just the selected class of device.




A convenient way to use the Devices window is to open it into a separate window using the Detach button on the main toolbar. This allows you to keep it available on your desktop at all times, even when you're working with other XMS windows (or other applications). (See “**Basic Window Operations**” on page 53).

The Devices window is automatically refreshed—you do not have to refresh it explicitly.

The Devices window has two sections:

- **Detected Devices**—a list of APs that have been detected.
- **Detecting Arrays List**—a list of the Arrays that detected selected devices.

You may resize the sections of the Devices window. Simply click and drag a horizontal border between sections to change their sizes. Columns may be resized by dragging the header separators.

You may customize both sections of the Devices window by changing the columns that are displayed and the order of display. If you prefer to use a smaller browser window for XMS and there's not enough room for all the columns to display, you can use this feature to select your preferred columns. Each of the sections has a **Select Table Columns** button  in the upper right corner. Click it to display the Table Column Chooser. The **Visible Columns** list shows the columns that will be displayed. Use the << and >> buttons to select the columns to display. Use the **Top**, **Bottom**, **Up** and **Down** buttons to arrange the columns, left to right. Click **Close** when done.

About Classifying Detected Devices

Every Xirrus Wi-Fi Array has a radio, abg(n)2, that (when configured to be in **monitor** mode) detects APs in its vicinity. If you set blocking on for one of these rogue APs, the Array's monitor radio sends out signals that will make it difficult for stations to associate to the rogue. Devices start out as **Unclassified** when first detected, and you may then *classify* them as **Blocked**, **Unknown**, **Known**, or **Approved**.

Classifying Rogue Devices via XMS

XMS allows you to classify rogue devices as Blocked, Unknown, Known, or Approved either individually or by using rules:

- individually—select a device from the **Detected Devices** list and click a button to specify its classification.
- **Enforced** rules are pushed (sent) to all managed Arrays to become part of the Arrays' Rogue Control Lists. If the Array has a conflicting rule (for the same wildcard pattern, but with a different classification), the XMS rule will replace the Array rule.
- **Unenforced** rules are not pushed to managed Arrays. This way, if an Array already has a rule for the same BSSID, SSID, or manufacturer, it will not be overridden.

Keeping unenforced rules in the database provides a single place where you can see a global view of all rules in the managed network, without necessarily applying all the rules universally. You may change a rule to Enforced if you wish.

XMS is the preferred tool for classifying rogue devices instead of classifying them using the Array's Rogue Control List, since XMS provides centralized administration.

Classifying Rogue Devices on Arrays

In the Array's Web Management Interface (WMI), the Rogue Control List window is used to classify rogue devices as Blocked, Known, or Approved. There are two ways to classify devices:

- individually—enter the BSSID (MAC address) of a device, and specify its classification.
- using a *wildcard* rule—enter the BSSID, SSID, or manufacturer of a device using an asterisk character (*) as a wildcard to match any string at this position. For example, 00:0f:7d:* matches any string that starts with 00:0f:7d:. Since Xirrus Arrays start with 00:0f:7d:, this applies the Rogue Control Type to all Xirrus Arrays.

Populating the XMS Devices Window

When the XMS server is first started, the Detected Devices list is empty, and there is one default rule: all Xirrus Arrays (BSSID 00:0f:7d.*) are Known. This rule is Enforced—it is sent out to all Arrays.

In order to populate the Detected Devices list, XMS fetches the rogue devices and Rogue Control List entries from each discovered Array. Thereafter during operation of XMS, Arrays are polled for new entries. Also during operation, when a new Array is discovered, XMS fetches its rogue devices and Rogue Control List entries and adds them to its database.

When a classification of an *individual device* is read from an Array and added to the XMS database it is marked as **Enforced**, and thus it will be “pushed” to all managed Arrays. On the other hand, when a *rule* is read from an Array and added to the XMS database, it is marked as **Unenforced**. This prevents the rule from being sent out to all managed Arrays, possibly overriding existing rules that were explicitly configured in Arrays. Once a rule has been added to the XMS database, if additional rules for the same BSSID/SSID are later read from other Arrays, they are ignored.

You may use the **Edit Rules** button at the bottom of the Detected Devices list to add new rules or edit existing rules. (For details, see “[Creating Classification Rules](#)” on page 126) If you set a rule to Enforced, it will be sent out to each managed Array and become part of its Rogue Control List.

Detected Devices

This section of the Devices window shows all of the potential rogue APs that have been detected by any of the Arrays in the Wi-Fi network.

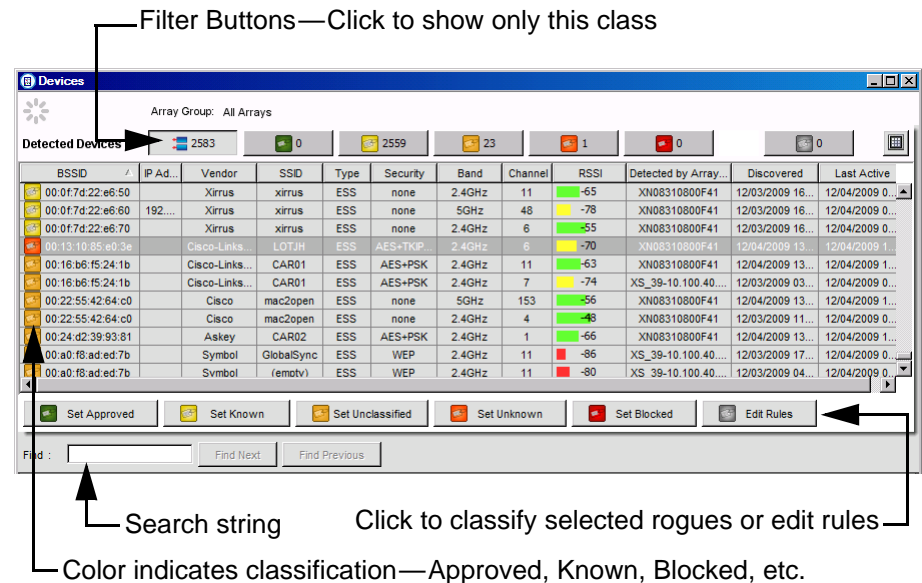


Figure 85. Devices Window—Detected Devices

Section Details

- **Filter Buttons**
The row of buttons along the top of this section shows a summary of the detected devices. The total count of devices detected is shown, along with the total in each class, represented by color. Hover the mouse over a button to display the name of the class—Known, Unknown, etc. Click a button to filter the list to show just the devices in that class.
- The classes and their representative colors are:
 - **Total:** This is the sum of the number of detected devices of all classes. Each rogue is counted in this list exactly once—even if it was detected by multiple Arrays. If you were previously viewing only entries of a particular class (for example, viewing only

Unknown devices), click this button to return to displaying all entries.

- **Green—Approved:** These are rogues that you have designated as Approved.
- **Yellow—Known:** These are rogues that you have designated as Known.
- **Gold—Unclassified:** When a device is initially detected, it is unclassified, which simply means that no one has classified it yet.
- **Orange—Unknown/Rogue:** These are rogues that you have designated as Unknown.
- **Red—Blocked:** These are rogues that you have designated as Blocked. If you classify a rogue AP as **blocked**, then the Array will take measures to prevent stations from staying associated to the rogue. When the monitor radio abg2/abgn2 is scanning, any time it hears a beacon from a blocked rogue abg2/abgn2 sends out a broadcast “death” signal using the rogue’s BSSID and source address. This has the effect of disconnecting all of a rogue AP’s clients approximately every 5 to 10 seconds, which is enough to make the rogue frustratingly unusable.
- **Gray—Ad Hoc:** An ad hoc wireless network is typically a network formed between two stations that are communicating with each other directly without going through a normal AP. This button shows a count of ad hoc nodes detected by Array APs.

Detected Devices List

All of the rogue APs detected in the XMS managed network are listed. This list is created as described in [“About Classifying Detected Devices” on page 120](#). The colored icon on the left of each entry shows its classification as listed above (Approved, Known, Blocked, Unknown, or Unclassified). Device identifying information is shown, including the BSSID and SSID broadcast by the rogue, its IP address (if any), its vendor (manufacturer), the channel that it is using, the **RSSI**, the security protocol in use, the Array that detected the rogue, and the time that it was detected. If the same physical device is detected by a number of Arrays, it will only be listed once in this table (under the detecting Array with the highest

RSSI). You may click on the header of any column to sort the entries by that column. Use the Classification Buttons (below) to classify a device.

Use the **Find** field to search the list for a device. Entries containing the search string in any position in any displayed column are found. The target entries need not start with the search string. The Find feature on this window works in the same way as searching for an Array in the Array window. See [“Using the Search Feature in the Resource Windows” on page 164](#).

Classification Buttons

These buttons allow you to set the security status of detected devices. We suggest that you use the following settings:

- Use **Set Approved** for devices in the operational network.
- Use **Set Known** for other devices not in the operational network but whose operation is known about, e.g., a neighbor or adjunct network.
- Use **Set Blocked** to counter rogues that you believe may be malicious.
- Use **Set Unknown** for other rogue or unapproved devices.
- **Set Unclassified**—when devices are first detected, they are unclassified. You may use this button to undo a classification that you previously applied.

When you classify a device as known, blocked, etc., that information is sent to every Array managed by XMS as soon as possible. Also, XMS sends its latest device classifications to all managed Arrays daily at 3 AM.

***NOTE:** Arrays have an Auto Block feature, which may be configured on the **Global RF Settings** policy window. There, you may set the **Auto Block Unknown Rogue AP** parameters so that when unknown APs are discovered, they will get the same treatment as explicitly blocked rogues.*

There are two ways to classify devices in this window—you may select one or more detected devices and use a button to set their classification, or you may set a rule to classify a group of devices (typically by manufacturer).

- To use a classification button, select an entry in the Detected Devices list and click one of the color-coded buttons at the bottom of the list to

classify the entry. You may select entries for multiple APs at the same time and click a button to apply the same classification to all of them. You may use **Set Unclassified** to remove a previously set classification (if any) from an AP. The changed classification will be displayed in the Devices window.

- To create a classification rule or to edit existing rules, see **Creating Classification Rules** below.

Creating Classification Rules

These rules allow you to classify groups of devices, rather than classifying each selected device individually. Rules may be enforced (pushed out to all Arrays) or unenforced, as described in **“Classifying Rogue Devices via XMS” on page 121**. Rules may be created as described below, or may appear as a result of being read from an Array (see **“Populating the XMS Devices Window” on page 122**). You may edit existing rules, if you wish.

To create or edit a classification rule, click the **Edit Rules** button on the right, below the **Detected Devices List**. The Device Classification Rules dialog box appears. (**Figure 86**)

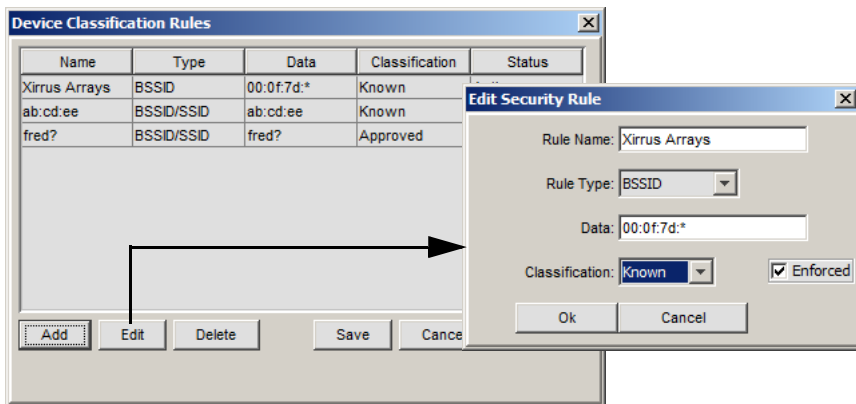


Figure 86. Editing Classification Rules

To add a new rule, click **Add**. In the Add New Security Rule dialog box, enter your **Rule Name**.

The **Type** field determines what to enter in the **Data** field as described below. The wild card character (*) may be used in the Data field for any of the types.

- **BSSID**—enter a MAC address (typically including * for a wild card) that describes the devices to be matched. When entering a MAC address, the string often specifies the OUI of a manufacturer—the first three octets of the device MAC address are a unique identifier for the manufacturer. For example, **00:0f:7d** is the OUI of Xirrus, so the string **00:0f:7d:*** will uniquely match all Xirrus Arrays.
- **SSID**—enter any legal SSID name to be matched. For example, to match the SSIDs named **xirrus-student** or **xirrus-staff**, enter the string **xirrus***.
- **BSSID/SSID**—either of the types above. This type is provided for backwards compatibility with rules that are read from some older Arrays. Note that rules created on newer Arrays have a **Match Only** setting that will specify either a BSSID or an SSID, although these Arrays will still process the old-style rules. On older Arrays, rules with type set to SSID, BSSID/SSID, or BSSID will all be processed on the Array as though they were BSSID/SSID rules. Rules with type set to Manufacturer will be dropped on older Arrays.
- **Manufacturer**—enter the manufacturer name as an ASCII string.

From the **Classification** drop-down list, select the classification to be applied to these devices. For example, you might set all Xirrus Arrays to **Known**.

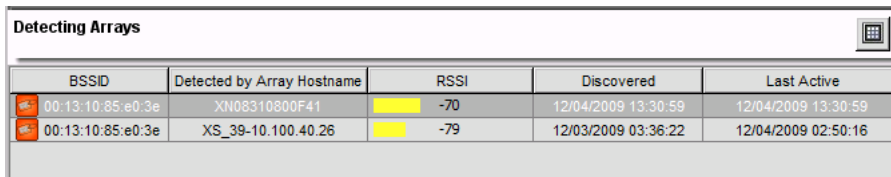
Leave the **Enforced** checkbox checked if you wish to have the rule pushed to all managed Arrays, otherwise clear the checkbox. See [“Classifying Rogue Devices via XMS” on page 121](#).

Click **OK** and then click **Save** when done.

To change an existing rule, select it in the list and click **Edit**, or to delete the rule click **Delete**.

Detecting Arrays List

This section of the Devices window shows the Array(s) that detected a selected rogue AP.



BSSID	Detected by Array Hostname	RSSI	Discovered	Last Active
00:13:10:85:e0:3e	XN08310800F41	-70	12/04/2009 13:30:59	12/04/2009 13:30:59
00:13:10:85:e0:3e	XS_39-10.100.40.26	-79	12/03/2009 03:36:22	12/04/2009 02:50:16

Figure 87. Devices Window—Detecting Arrays

To use the Detecting Arrays list, select an entry from the **Detected Devices List** in the top half of the window. All of the Arrays that detected the selected AP will be shown in the Detecting Arrays list. You may select multiple APs—in this case, the detecting Arrays for each selected AP will be included.

Section Details

- **Detecting Arrays List**

For each rogue AP selected in the **Detected Devices** list, there is an entry for each Array that has detected that AP. Thus, if the AP has been detected by three Arrays, there will be three entries for the AP in this list. Each entry identifies the AP by its BSSID and shows the Array that detected it, along with the **RSSI** of the detected signal, and the time that it was detected. You may click on the header of any column to sort the entries by that column.

Working with Maps

This chapter takes you on a tour of the Java client's map window and its features. It offers a procedure for creating your own custom map, and shows you how to display a contour map of your RF coverage. Section headings for this chapter include:

- [“About Maps” on page 129](#)
- [“Getting Started with Maps” on page 130](#)
- [“The Map Window” on page 132](#)
- [“Migrating Maps from Earlier Releases” on page 142](#)
- [“Preparing Background Images for New Maps” on page 142](#)
- [“Adding a New Map” on page 144](#)
- [“Saving a Map \(Important!\)” on page 145](#)
- [“Setting the Map’s Scale” on page 146](#)
- [“Adding Arrays to Maps” on page 147](#)
- [“Orienting Arrays” on page 150](#)
- [“Entering Environment Settings” on page 151](#)
- [“Locating Devices” on page 152](#)
- [“Changing Contour Map Colors” on page 156](#)
- [“Deleting a Map” on page 157](#)
- [“Managing Arrays Within Maps” on page 158](#)
- [“Map Settings Window” on page 160](#)

About Maps

Maps offer a topographical view of your network and all Wi-Fi Arrays contained within the network. From any map view you can drill down to specific Arrays and organize how your network is represented in the Java client interface.

A contour map shows Wi-Fi coverage at your site, and is based on measurements observed by Arrays. It visualizes the RF environment provided by your Wi-Fi network. The map incorporates directional antenna coverage on a per radio basis,

and readings are enhanced by means of inter-Array correction. By leveraging the RF analysis capabilities available on the Array, XMS makes it easy to view the changing RF environment.

The XMS Locationing capability displays the position of a device on the map for you, facilitating asset tracking and security policy enforcement.

Getting Started with Maps

This overview describes how to get started using maps, and points you to topics that describe each step in detail.

- **“The Map Window” on page 132**—provides an overview of the map window. To display the map window, select **Resources > Locations** from the **Tree** on the left of the XMS Java client.
- **“Migrating Maps from Earlier Releases” on page 142**—XMS is furnished without any default maps. However, if you have already created maps in pre-5.0 releases of XMS, they will automatically be migrated to the current release.
- To add a new map (and modify existing ones):
 - **“Preparing Background Images for New Maps” on page 142**—you must supply a background image for your map, such as a floor plan or a site layout of buildings.
 - **“Adding a New Map” on page 144**—follow these instructions to create a new map.
 - **“Saving a Map (Important!)” on page 145**—be sure to save the new map, and save again after making changes.
 - **“Setting the Map’s Scale” on page 146**—set the distance scale for the map, so that RF contours will display accurately.
- Select the Arrays that belong on the map. See **“Adding Arrays to Maps” on page 147**.
- Rotate each Array on the map so that the **abg(n)2** radio has the correct orientation. See **“Orienting Arrays” on page 150**.

- Set the typical RF signal attenuation for the type of construction in the mapped area. See **“Entering Environment Settings” on page 151.**
- After completing the steps above, you may use the RF Heat Map to present a live display of RF coverage by Array. To manage Arrays, see **“Managing Arrays Within Maps” on page 158.**
- You may customize your display if you wish. See **“Changing Contour Map Colors” on page 156** and **“Map Settings Window” on page 160.**

The Map Window

To display the map window, select **Resources > Locations** from the **Tree** on the left of the XMS Java client. The map window will be displayed in the **Main Viewing Area** of the client interface. Select the desired map from the Map List.

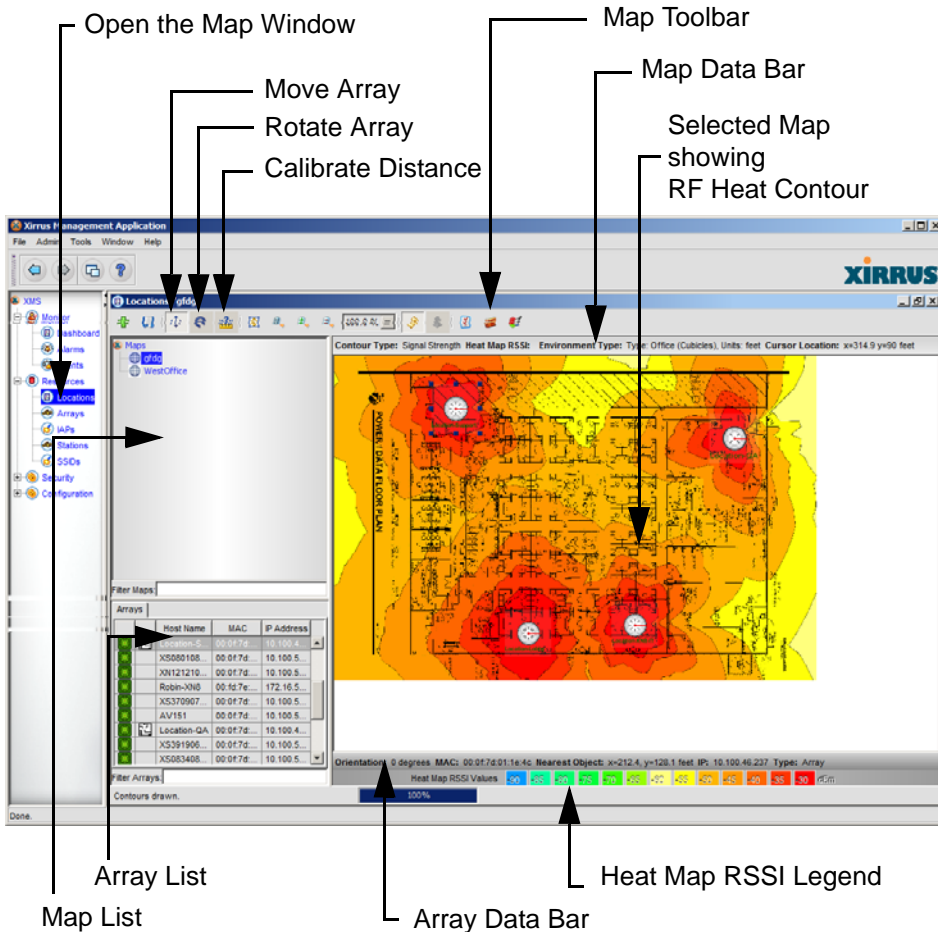


Figure 88. Main Map with RF Heat Contours Enabled

The map shows all Arrays that have been explicitly placed on it (see **“Adding Arrays to Maps” on page 147**), offering a convenient view of the Arrays.

No default maps are provided in XMS 5.0. If you have created maps in a previous release of XMS, they will be present after you upgrade. When you first upgrade to 5.0 and later releases, maps created in a pre-5.0 release of XMS will be automatically migrated. See [“Migrating Maps from Earlier Releases” on page 142](#). You may create new maps as described in [“Adding a New Map” on page 144](#).

The map window has the following parts:

- **The Map List**
- **The Arrays List**
- **The RF Heat Contour Map**
- **Map Toolbar**
- **Information Bars**

The Map List

This list shows all of the maps in the XMS database. Click on a map to display it. If the currently displayed map has unsaved changes, you will be asked whether to save the changes before the new map selection is displayed.

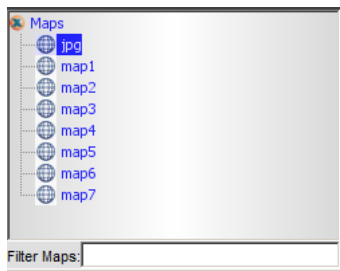

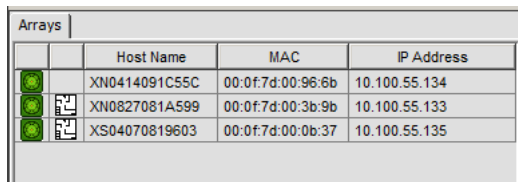


Figure 89. The Map List

You may use the **Filter Maps** field below the list to help find a map. Type in any string that appears anywhere in the name of the desired map(s). As you type, XMS narrows the Map List to maps that contain that string. To return to showing all maps, just clear the **Filter Maps** field.

The Arrays List

This list shows all of the discovered Arrays in the XMS database. The first column indicates Array status, and a “mapped” icon  in the second column indicates that the Array has been added to one of the maps. (It does not mean that the Array has been added to the currently displayed map.) You may sort the entries by clicking on the header of any column: **Host Name**, **MAC Address**, **IP Address**, or the status or “mapped” icons. Click again to reverse the sorting.









	Host Name	MAC	IP Address
 	XN0414091C55C	00:0f:7d:00:96:8b	10.100.55.134
 	XN0827081A599	00:0f:7d:00:3b:9b	10.100.55.133
 	XS04070819603	00:0f:7d:00:0b:37	10.100.55.135

Figure 90. The Arrays List

Any Array that is not already a member of a map may be easily added to the current map by selecting and dragging it onto the map. See [“Adding Arrays to Maps” on page 147](#). An Array may belong to only one map at a time.

Searching for an Array in the Arrays List

To find an Array in the list, click anywhere in the Arrays List and type **Ctrl+f**. In the **Find** field, enter the string that you wish to match. Click the **Find** button, and XMS will highlight the next list entry that contains that string in any position in any column. Click again to jump to the next matching entry.

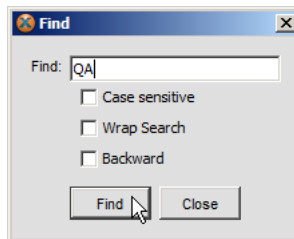


Figure 91. Finding an Entry in the Arrays List

Searching for an Array on the Map

To find the location of an Array on any map, double-click the Array in this list, or right-click it and select **Locate** from the menu. This displays the map that contains that Array (if different from the current map), and selects the Array on the map.

You may use the **Filter Arrays** field below the list to help find an Array. Type in a string that appears in any position in any of the displayed columns of the desired Array(s). As you type, XMS narrows the Arrays List to entries that contain that string (the search is not case-sensitive). To return to showing all Arrays, just clear the **Filter Arrays** field.

The RF Heat Contour Map

The heat map gives an at-a-glance representation of the Arrays in an area, their locations, and the RF coverage that they provide. Areas of low coverage are immediately visible. You may right-click on an Array to display a menu of options for managing it. Use [The Arrays List](#) to easily locate an Array.

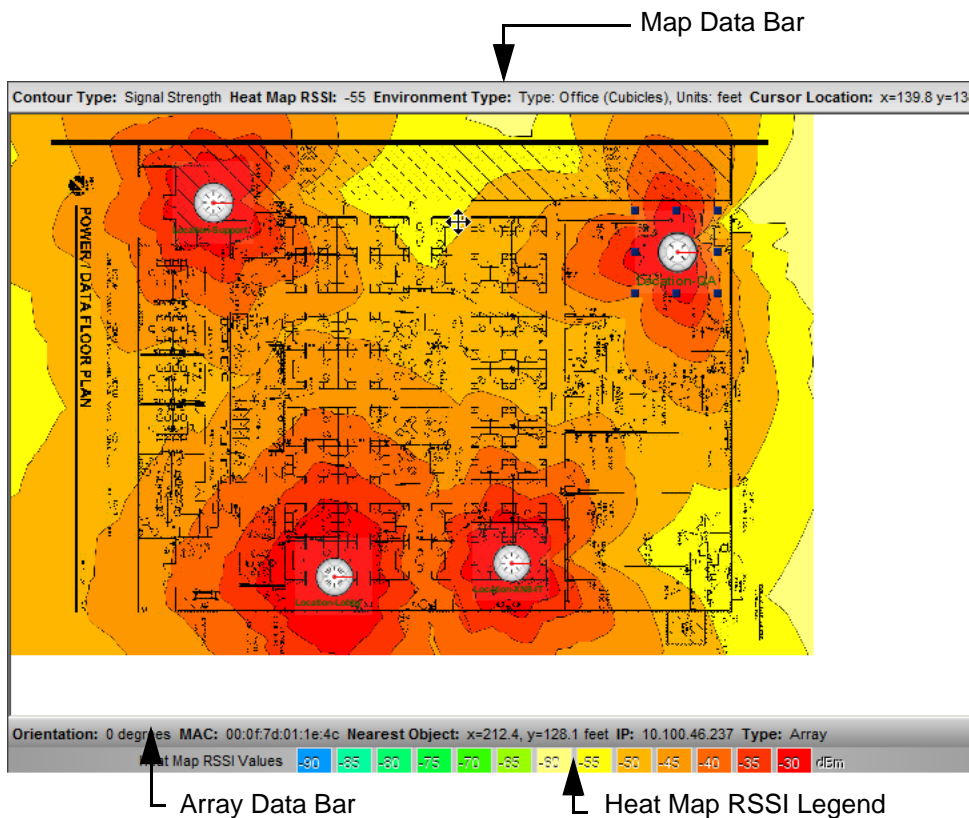



Figure 92. Main Map Showing RF Heat Contours




When the Display Contours button  is enabled, the RF contours displayed on this map show the intensity of RF signals broadcast by each Array's radios. If an Array's radios are disabled, no contours are displayed for that Array. Signal strength is displayed using the colors shown in the Heat Map RSSI Values legend

under the map. You may change these colors if you wish—see [“Changing Contour Map Colors” on page 156](#). You may also change the transparency of the colors (the degree to which the map is still visible). See [“Map Settings Window” on page 160](#).

The management operations available in the heat map window depend on your XMS account privileges. If you have logged in to XMS using a read only account, you cannot make any modifications to the map. For example, you may not add Arrays to the map, move them, or remove them. Read-only users also cannot add or delete maps, or change any map settings such as the scale or environment settings. A read-only user can select an Array on the map or in the Array list and use the right click menu to display information, but no configuration options are enabled—only **Web Management**, **Array Status**, **Alarms and Events**, **Reports**, and **Refresh** are available. You may perform operations which change your view of the map, such as zooming in and turning contour display on and off.

Map Modes of Operation

XMS users with read-write privileges may perform any operation on a map. Maps have three modes of operation, depending on the mouse tool that you select:

-  **Move Array (Normal) Mode:** This is the default mode, and is the one that you will use almost all of the time. This mode is used for placing Arrays on maps, moving them, and using the right click Array menu. Enter this mode by clicking the button for the Move Object tool in the map toolbar. Only administrators with read/write privileges may use this mode.
-  **Rotate Array Mode:** Use this mode to set the orientation of an Array on the map. See [“Orienting Arrays” on page 150](#).
-  **Calibrate Distance Mode:** Use this mode to set the scale of the map. See [“Setting the Map’s Scale” on page 146](#).

After using the Rotate Array tool or the Calibrate Distance tool, you will typically want to click the Move Array button again to resume normal use of the map.

The appearance of the map may be customized in the following ways:

- Set the map's scale—see [“Setting the Map's Scale” on page 146.](#)
- Specify RF signal attenuation for your type of construction—see [“Entering Environment Settings” on page 151.](#)
- Set the level of opacity of the heat contours that are superimposed on the map—see [“Map Settings Window” on page 160.](#)
- Change the colors used in the contour map to represent levels of signal strength—see [“Changing Contour Map Colors” on page 156.](#)

The following sections discuss the **Map Toolbar** and **Information Bars**.

Map Toolbar

This toolbar provides functions for managing and viewing maps.

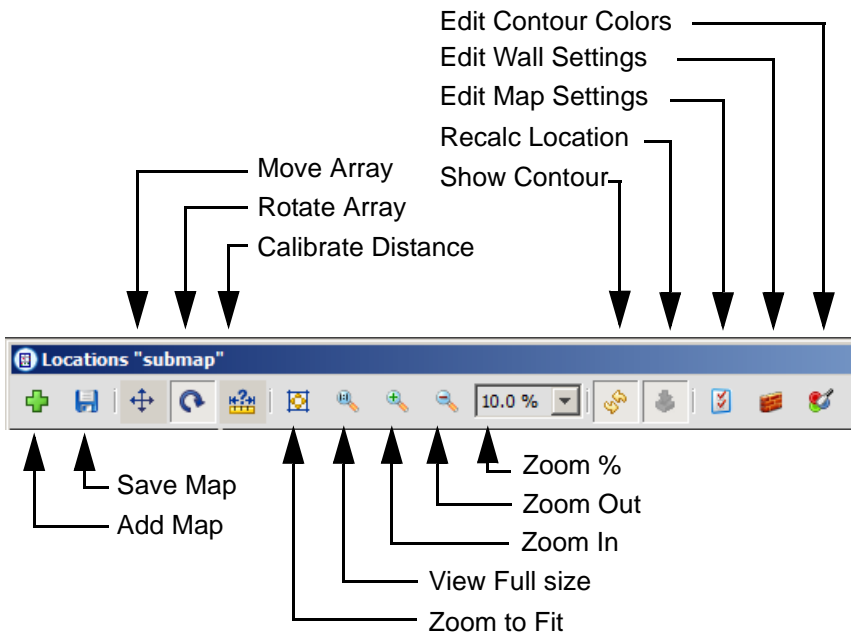


Figure 93. The Map Toolbar

The following buttons are available, from left to right:



Add Map

Click to create a new map, as described in [“Adding a New Map” on page 144](#).



Save Map

Click to save changes to a map, as described in [“Saving a Map \(Important!\)” on page 145](#).



Move Array

Allows you to move, delete, or manage Arrays on the map. This tool is active by default. See [“Map Modes of Operation” on page 137](#).



Rotate Array

Click to set the orientation of Arrays. See [“Orienting Arrays” on page 150](#).



Calibrate Distance

Click to set the scale. See [“Setting the Map’s Scale” on page 146](#).



Zoom to Fit

Click to zoom the view so that the entire map fits in the current window size.



Show Full Size

Click this to zoom the view to 100%, i.e., zoom to the full size of the map background image file.



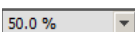
Zoom In

Click to enlarge the map display size.



Zoom Out

Click to reduce the map display size.



Zoom Percentage

Enter a desired map display size in the field, or select a zoom value from the drop-down list.



Display Contour

Click to turn the display of heat map contours on or off.



Recalculate Location

After using **Locating Devices** to find the position of a station, use this button to hide the location or recalculate and show the position.



Edit Map Settings

Click here to select the data displayed on the **Information Bars**. See **“Map Settings Window” on page 160**.



Edit Environment Settings

Click here to describe the construction in your environment and the RF signal attenuation expected at your site. See **“Entering Environment Settings” on page 151**.



Edit Contour Colors

Click here to change the colors that are used to represent RF signal strengths on the heat contour map. See **“Changing Contour Map Colors” on page 156**.

Information Bars

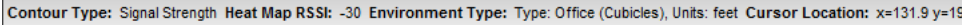
Information about your *current position* on the map (i.e., the current position of the mouse pointer) is displayed in bars above and below the heat map, as shown in **Figure 92 on page 136**. This allows you to investigate different areas of the map without changing your current Array selection. To customize the information displayed, see **“Map Settings Window” on page 160**.

The following sections describe the Information Bars:

- **“Map Data” on page 141**
- **“Array Data” on page 141**

The bottom of the map also has a Heat Map Signal Strength Values legend, which defines the signal strength indicated by each color. You may change these colors if you wish—see **“Changing Contour Map Colors” on page 156**.

Map Data



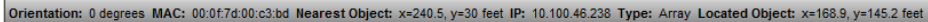
Contour Type: Signal Strength Heat Map RSSI: -30 Environment Type: Type: Office (Cubicles), Units: feet Cursor Location: x=131.9 y=15

Figure 94. The Map Data Information Bar

The Map Data bar is displayed above the heat map. Depending on your settings in the **Map Settings Window**, the following values may be shown for the mouse pointer's current location, updated as the mouse moves:

- **Contour Type**—the type of measurement that the contours are based on. This value is always Signal Strength.
- **Heat Map RSSI**—the RF signal strength at the current location.
- **Environment Type**—this displays the wall settings defined for the map in **"Entering Environment Settings" on page 151**.
- **Location**—the mouse pointer's position on the map, expressed in terms of feet from the lower left corner of the map. The distance is calculated based on the scale set in **"Setting the Map's Scale" on page 146**.

Array Data



Orientation: 0 degrees MAC: 00:0f:7d:00:c3:bd Nearest Object: x=240.5, y=30 feet IP: 10.100.46.238 Type: Array Located Object: x=168.9, y=145.2 feet

Figure 95. The Array Data Information Bar

The Array Data bar is displayed below the heat map. If you have been **Using the Location Feature**, then this shows information about the station that was located and about the Array or located station that is closest to the mouse. Otherwise, it shows information about the Array that is closest to the mouse pointer's current location, updated as the mouse moves (it shows information about the nearest Array, rather than the currently selected Array). You will notice that the values shown remain unchanged until the mouse moves closer to a different object. Depending on your settings in the **Map Settings Window**, the following values may be shown for the nearest Array:

- **Orientation**—the angle of the nearest Array's abg(n)2 radio, measured from the horizontal (x) axis, or 0 if the nearest object is a located station.
- **MAC**—the MAC address of the nearest Array.

- **Located Object** or **Nearest Object**—If you have been [Using the Location Feature](#), then **Located Object** shows the position of the station on the map, expressed in terms of feet from the lower left corner of the map. The distance is calculated based on the scale set in [“Setting the Map’s Scale” on page 146](#). **Nearest Object** shows the position of the nearest Array.
- **IP**—the IP address of the nearest Array or located station.
- **Type**—Array or located Station.

Migrating Maps from Earlier Releases

When you upgrade your XMS server from a version earlier than Release 5.0 to a Release 5.0 or later version, any maps that you have already created are automatically migrated to new maps that are compatible with the XMS release being installed. They are immediately available for use with the new software. Migrated maps will be listed in the **Locations** section of the [Tree](#) under the same names that they previously had.

Note that the old (pre-5.0 release) map information is kept in the XMS database. If you should wish to revert to an older release of the server, the old-style maps will still be available.

Before you begin using a migrated map be sure to perform these steps so that the map will accurately represent your environment:

- [“Setting the Map’s Scale” on page 146](#).
- [“Entering Environment Settings” on page 151](#)

Preparing Background Images for New Maps

You will typically want to present maps with a background image such as a floor plan or a site layout of buildings, a geographic area, a functional domain within your corporation, or any combination of map designs—whichever suits your needs.

XMS will accept most graphic file formats for your background images, though we recommend using either GIF, PNG, JPG, or JPEG (these formats are the most suitable for online use). In particular, whenever possible, optimize your image

files and try to keep the file size between 50KB and 100KB. Files in this size range will load into the client quickly, give reasonable image resolution, and will perform well when zooming in.

Preferred Image Formats

- **GIF (Graphics Interchange Format)**
This is the file format most commonly used to display indexed-color graphics and images in HTML documents over the Web and other online services. Simple graphics (for example, floor plans) with or without spot colors are considered most suitable for the GIF file format, which is designed to minimize the image file size and electronic transfer time.
- **PNG (Portable Network Graphics)**
This format is an alternative to the GIF format but supports 24-bit images with “no loss” compression and produces background transparency without jagged edges. However, some older Web browsers do not support this format.
- **JPEG (Joint Photographic Experts Group)**
This format is commonly used to display photographs and other continuous-tone images. Unlike GIF images, the JPEG format retains all color information in an RGB graphic, but compresses the file size by selectively discarding data without serious degradation to the quality of the original image.

Physical Size

The physical size of the image is not critical because XMS scales the image automatically. However, the more scaling that is required the greater the loss in quality. We recommend a physical size of between 10 inches and 14 inches wide, while maintaining the aspect ratio of the original image (when scaled, the vertical axis will retain the correct proportion with the horizontal axis).

Resolution

The preferred resolution for your map background images is 72 dpi (standard for online viewing). A higher resolution will generate a smoother image, but the file size will be increased relative to the resolution you choose.

Adding a New Map

XMS allows you to add maps. Existing maps are displayed in the **Maps** list.

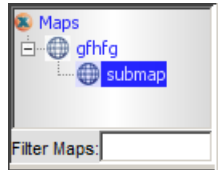



Figure 96. Maps List

To add a new map, use the following procedure:

1. Use any common graphics application to create a background image for your map. The image file should be optimized for the smallest size possible. For more information about creating background images, go to [“Preparing Background Images for New Maps” on page 142.](#)
2. In the map window, if this is to be a top level map, then click Maps in the Maps List. If it is to be a submap of an existing map, click that existing map in the Map list. Then click the **Add Map** button  towards the left on the **Map Toolbar**. (You do not need to be in “Move Array” mode to add a map.) The Map Settings window is displayed.

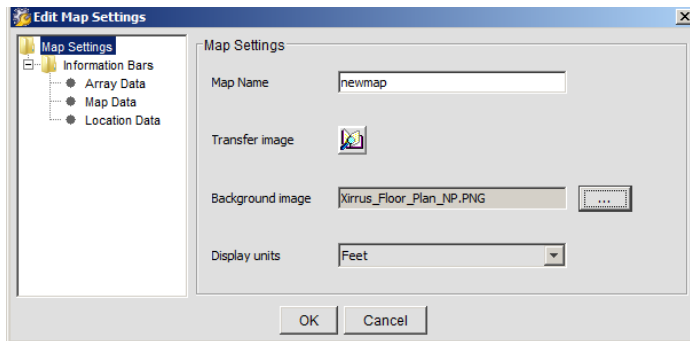






Figure 97. Map Settings Window

3. Enter a name for the new map in the **Map Name** field. Click the **Transfer Image** button  and browse to select the image file. Note that the file should be located on your file system (accessible from the computer where you are running the XMS client), and the filename may not contain any spaces. Click **Upload**.

The file is uploaded to the proper folder on the server. It may be used as a background for any map. Click the  button to the right of the **Background Image** field to select the uploaded image file.
4. Select the desired **Display Units** (feet or meters), and click **OK** to create the new map.
5. Click the **Save Map** button. 
6. You may modify a map. Click the **Edit Map Settings** button  on the map toolbar, or right click the map in the **Maps** list and select **Properties** from the drop-down menu. You may change the **Background Image**, **Display Units**, or even the **Map Name**.


You can now start to build your map by performing these steps.

- [“Setting the Map’s Scale” on page 146](#)
- [“Adding Arrays to Maps” on page 147](#)
- [“Orienting Arrays” on page 150](#)
- [“Entering Environment Settings” on page 151](#)

To work with the Arrays that you have placed on the map, see [“Managing Arrays Within Maps” on page 158](#).

Saving a Map (Important!)

Always remember to save your map after making changes, since many map features will not be up to date until you save the map. For example, you cannot access the right-click menu for a recently added Array on the map until it has been saved. The map Arrays list will not show a map icon for the Array, nor will the right-click Locate feature work until you have saved.

To save a map after making changes, click the **Save Map** button.  Saving your map makes it available to all users of the XMS server.

XMS will prompt you to save the map before it will allow you to switch to another map page or close the Java client.

Setting the Map's Scale

It is important to set the scale of each map in order for the RF heat map contours to display accurately and for location information to be as precise as possible.

It is very easy to set the scale. Before you start, measure the actual length of a wall or other feature represented on the map. The longer the object being measured is, the more accurate the scale will be.

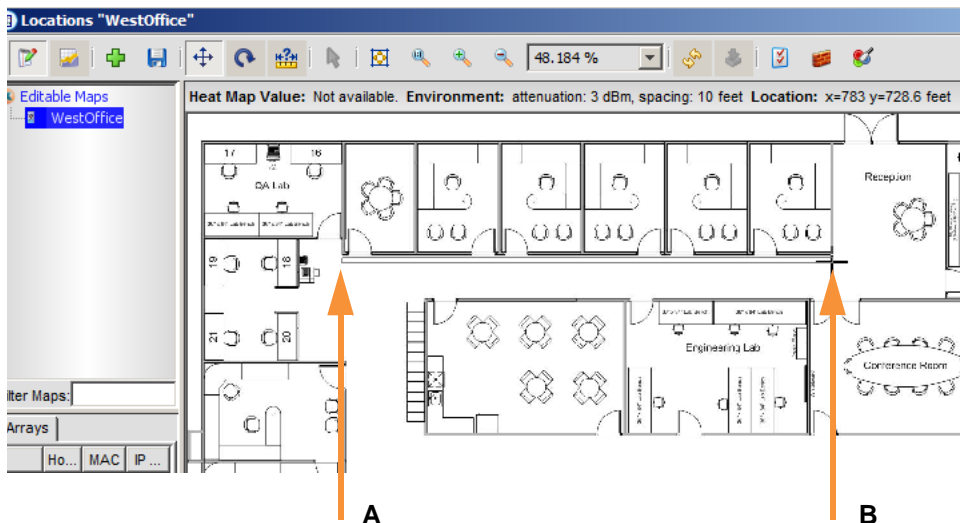



Figure 98. Calibrating the Map Scale

1. Measure a wall or other feature that is represented accurately on the map. **Figure 98** shows both ends (A and B) of a wall being measured.
2. Click the **Calibrate Distance** button.  The mouse pointer will change to a calibration tool in the next step.

3. On the map, move the cursor to one end of the wall or other feature that you measured (A). Click and drag the mouse to draw a line to the other end of the feature (B). Release the mouse button.

The Edit Calibration dialog box appears.

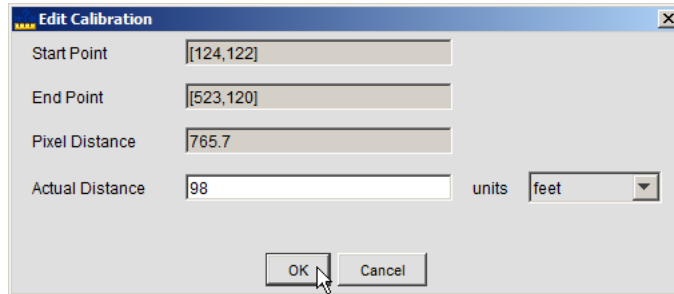



Figure 99. Edit Map Scale (Calibrate Distance)

4. Set **Actual Distance** to the measured length of the feature. Click **OK**.
5. The pointer continues to be a calibration tool until you change it to another tool such as the move or rotate tool.
6. Click the **Save Map** button to save your work. 


Adding Arrays to Maps

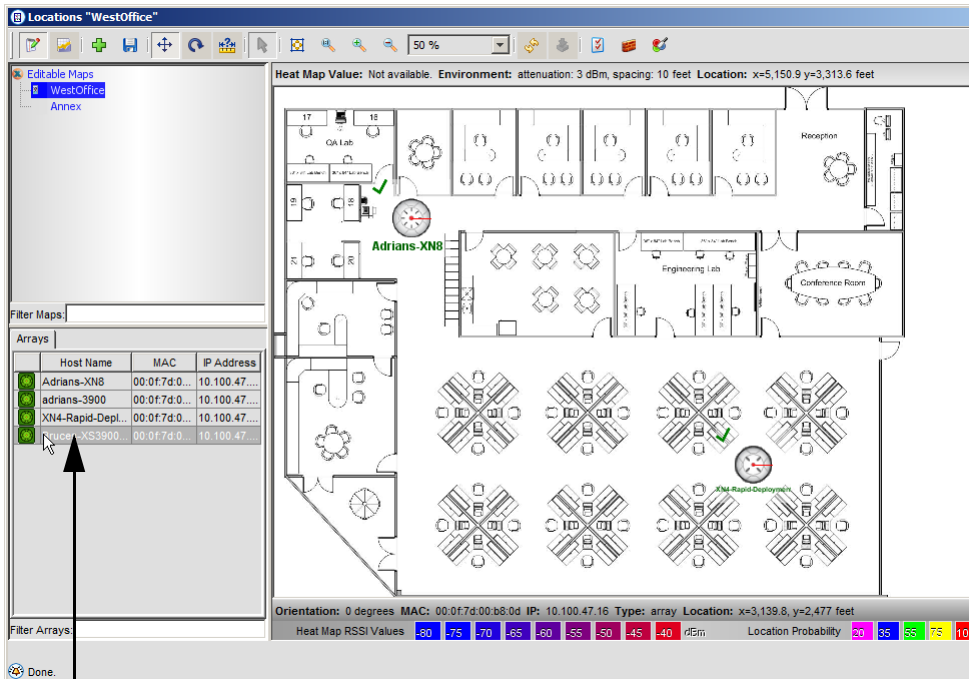
After you create a map and set its scale, the next step is to drag and drop Arrays onto the map, locating them to match their physical locations as closely as possible. Each Array may only belong to one map at a time.

The procedure below describes how to add an Array to the map, resize its icon, move it, or delete it.

To add an Array to the map, use the following procedure.


1. Click the **Move Object** button.  You must use the Move Arrays tool to drag Arrays onto the map.

2. Find a desired Array in the **Arrays List** as shown in **Figure 100**. If the Array already belongs to another map as indicated by the “mapped” icon  in the second column icon, you will need to remove it from that map before adding it to another map (see **Step 7** below).
3. Click to select the Array from the list. Click again and drag and drop it onto the desired map location.



Drag and drop selected Array onto the map in the desired location

Figure 100. Adding an Array to a Map

4. Click the **Save Map** button to save your work. 
5. To resize the Array icon, click it. Then position the mouse over one of the drag handles (black squares at corners and in the middle of each side) and drag it to enlarge or reduce the size of the Array symbol. (**Figure 101**)

6. To move an Array, click it. Then position the mouse anywhere except over a drag handle. Drag the Array to the desired position. (Figure 101)
7. To remove an Array from the current map (without deleting it from the XMS database), do one of the following:
 - Select the Array on the map or in the Arrays list, and then use the Delete button on your keyboard.
 - Select the Array and right-click. Select **Remove from Map** from the drop-down menu. Do **not** select **Delete** from the menu—this will remove the Array from the XMS database!
 - You may select multiple Arrays by using Ctrl + click, and then remove them in one step by using the Delete button on the keyboard.

Remember to click the **Save Map** button to save your work.  This will update the Arrays list with your changes as well.

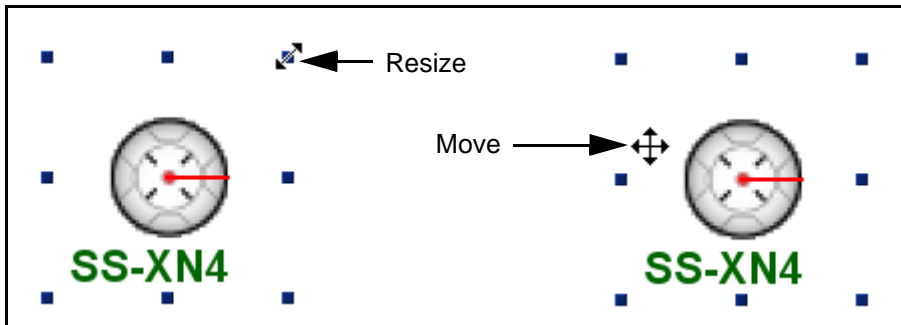



Figure 101. Resizing and Moving Arrays

Orienting Arrays

After adding an Array, you must rotate it on the map to match the actual orientation of its abg(n)2 radio. This is critical for accurately calculating and displaying locations of stations. This also allows the heat contours to be correctly displayed on the map.

To rotate an Array on the map, use the following procedure.

1. Click the **Rotate Array** button. 
2. Click to select the desired Array on the map.
3. Click the red Orientation Line on the selected Array and drag it to the desired angle. Note that the Orientation Line gets longer when you drag it, and the new angle is displayed as you rotate. The angle is measured from the horizontal (x-axis) in the same way as on a graph. The angle may be changed in increments of 22.5 degrees—for example, the angle may be increased in four steps going from 0 to 90 degrees.

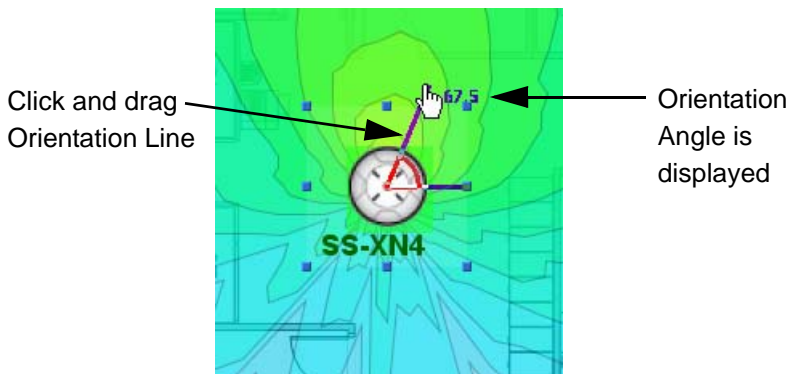


Figure 102. Rotating an Array

4. Click the **Save Map** button to save your work. 

Entering Environment Settings

Environment settings customize your map for the type of construction in the area represented by the map. XMS uses these values to determine the degree of RF signal attenuation at your site. This is required for using the Location feature, and increases the accuracy of RF heat map contours. See the discussion of “Planning your Installation - General Deployment Considerations” in Chapter 2 of the *Xirrus Wi-Fi Array User’s Guide*.

1. Click the **Edit Environment Settings** button.  The Edit Environment Settings dialog box appears.

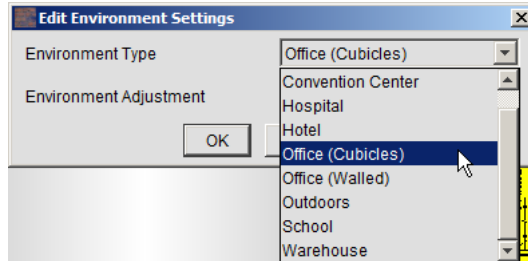



Figure 103. Entering Environment (Wall) Settings

2. Select the typical **Environment Type** for your type of construction, for example, **Office (Cubicles)**, **Office (Walled)**, **School**, or **Warehouse**.
3. Now, use **Environment Adjustment** to tune the environment settings for the area included in the map. To set the adjustment properly, you should take a few data points and compare them to the values on the heat map without any adjustment. If the heat map shows -75dB at a particular spot but your reading is -70dB, then you should set an adjustment of +5dB. Likewise, if the map shows -50dB, but your measurement is -55dB, then set an adjustment of -5dB. Click **OK** when done.
4. Click the **Save Map** button to save your work. 
5. You may click the **Edit Environment Settings** button again if you need to modify these values.

Locating Devices

The XMS Locating feature leverages the RF capability of the Wi-Fi Array to determine the position of a device to within a few meters and display it on the map. With this capability, you can track assets using your existing Wi-Fi infrastructure. Locationing is available for stations that are associated to an Array that is a member of a map.

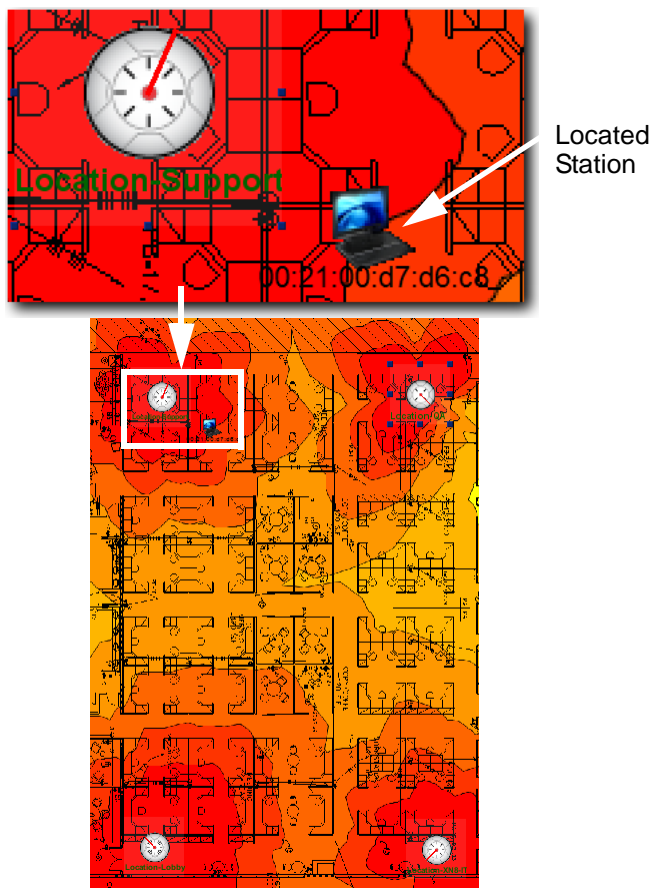


Figure 104. Using the Location Feature

The location feature is described in the following sections:

- **Understanding Locationing**
- **Preparing to Use Locationing**
- **Using Locationing**

Understanding Locationing

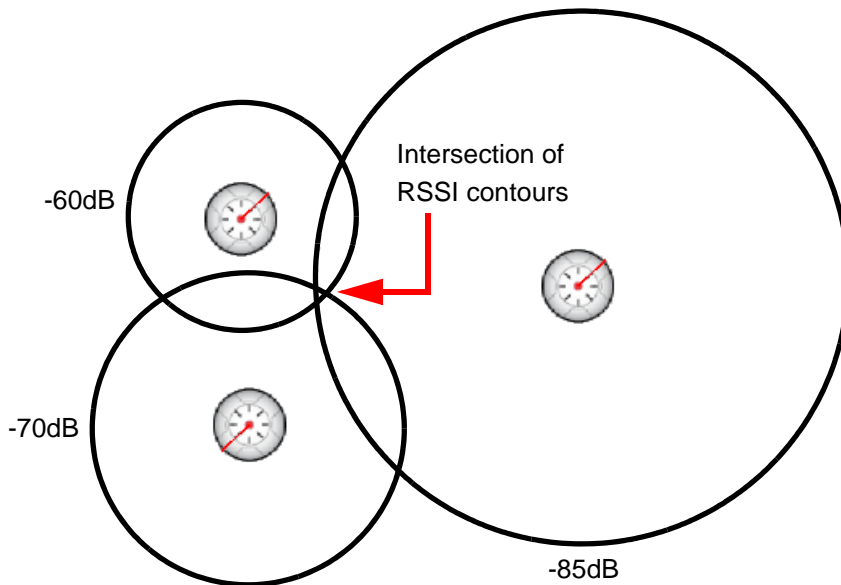


Figure 105. Determining Position

XMS uses a technique called trilateration based on received signal strength to determine the location of a selected wireless client. When you request the location of a station, each Array that can hear the station's signal reports back, giving the received signal strength. The signal strength indicates the approximate distance of the station from the Array. A simplified representation of this is illustrated in **Figure 105**, showing the RF contour of the observed signal strength as a circle around the Array. Each circle shows possible locations of the station, based on that Array's signal strength observation. In the diagram, if there were only two Arrays reporting, the circles would intersect at two points, giving two possible

locations for the station. When you add additional Array observations, the intersection of the circles defines the station's most likely location. Actually, XMS has much more information than a simple radius (circle) to work with, due to the advanced design of the WiFi Array. The Array's multiple directional radios also give information on the direction of the station. Rather than modeling the location of the station as a circle, the RF contour map is used. This map incorporates directional antenna coverage on a per radio basis, and readings are enhanced by means of inter-Array correction and take RF attenuation due to building construction into account.


Preparing to Use Locationing

You must complete the following steps before locating a device to get the best results.

- **Planning**—XMS is able to locate a device most accurately when Arrays are located around the perimeter of the area to be monitored, as shown in **Figure 104 on page 152**. This is in contrast to placement of Arrays for greatest Wi-Fi coverage, where we recommend that you place Arrays away from exterior walls.
- **Adding a New Map**—Create an XMS map, using the most accurate graphic representation possible.
- **Setting the Map's Scale**—It is very important to set this accurately, as the placement of a located device depends critically on the scale of the map.
- **Adding Arrays to Maps**—As you place your Arrays on the map, be certain to get their locations as precise as possible. XMS will only locate stations that are associated to an Array that is a member of a map.
- **Orienting Arrays**—The orientation of the Arrays must also be as accurate as possible.
- **Entering Environment Settings**—Set this according to the type of construction at your deployment site.

Using Locationing


The XMS location algorithm will locate a selected station that is associated to an Array on a map.

1. Go to the **Resources > Stations** window in the Java client.
2. Select the station that you wish to locate and right-click it. Select **Locate** from the drop-down menu.
3. XMS determines which map contains the Array to which the station is associated. That map window will be displayed, and the location of the station is displayed. See **Figure 104 on page 152**.
4. If the associated Array is not a member of any map, an error message will inform you of this problem. You must add the Array to a map in order to locate the stations that are associated to it.
5. If you wish to toggle between hiding or refreshing and redisplaying the station location, click the **Recalculate Location** button. 

Only one station location may be displayed at a time.

Changing Contour Map Colors

The **RF Heat Contour Map** displays signal strength available over the area covered by your map. Colors are used to show the gradients of strength. You may select one of the predefined color sets for the contour map, or you may change the colors displayed or completely customize them using the procedure that follows.

1. Click the **Color Settings** button.  The Edit Contour Colors dialog box appears. (Figure 106)

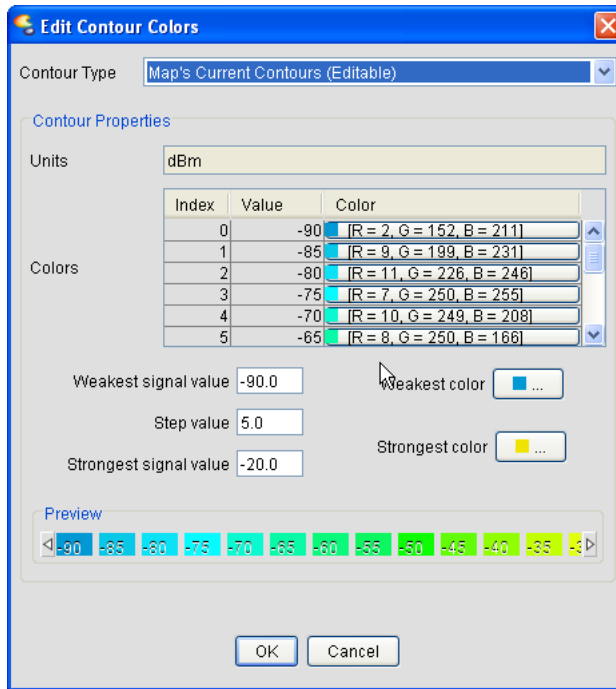


Figure 106. Changing Contour Map Colors

2. Select the desired color set from the **Contour Type** field. The Preview section at the bottom of the dialog box shows the colors that will be displayed by the settings you have chosen, along with the RF value represented by each color.

- You may simply change any of the signal strength values that are associated with the colors shown. Double-click an entry in the **Value** column, and enter the desired RSSI value. Click **OK** when done changing values. You should see your new values displayed in the **Heat Map RSSI Values** legend at the bottom of the map.
- 3. You may not save modifications to any of the predefined color schemes, but you may edit the current working colors.

To customize your own color set:

- In the **Contour Type** field, select **Map's Current Contour Colors (Editable)**.
 - You may simply change any of the signal strength values that are associated with the colors shown, as described in [Step 2](#).
 - To create your own color scheme, first specify the range of values to be represented. Enter the **Weakest signal value**, the **Strongest signal value**, and the **Step value** (5 or greater) for increments in between the two ends of the range.
 - Next you may specify the range of colors by selecting the **Weakest color** and the **Strongest color**.
4. Click the **OK** button to return to the map. Your changes will be saved for this map only.

Deleting a Map

If you delete a map, the map is permanently removed from the database. Make sure you want to permanently delete the map before doing so.

1. To delete a map, right-click it in the **Maps** list on the left and choose **Delete Map**. When prompted, click on the **Yes** button to delete the map.

Managing Arrays Within Maps

Each discovered Xirrus Wi-Fi Array may be displayed in maps as a graphical representation of the Array itself, labeled with the Array's host name (if it is unique) or IP address. If an Array does not have a unique IP address, then its MAC address is shown. The example in [Figure 107](#) shows an Array icon with its host name, as displayed in any map window.

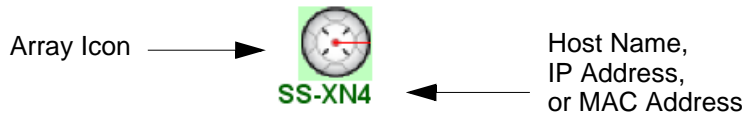


Figure 107. Displaying Arrays Within Maps

This section only deals with managing the Array icons within the map and basic Array operations. It does not cover Array properties or configuring Arrays. For this and other Array information, go to [“Arrays” on page 165](#).

Most Array management is performed by right-clicking an Array on the map or in the Arrays list on the lower left. ([Figure 108](#)) This menu is identical to the drop-down menu that appears when you right-click an entry in the [Arrays](#) window. It includes functions such as connecting to the Array's Web Management Interface (WMI), configuring the Array via XMS, creating policies from the Array, and more. For details on all of these, please see [“Array Operations” on page 170](#).

Some of the menu options are targeted for the map window:

- **Remove from Map**

Use this to remove the selected Array from the map. You will need to save the map to have the change reflected in [The Arrays List](#) and make the change permanent. This menu choice does not remove the Array from the XMS database—if you wish to do this, use the **Delete** option instead.

- **Locate**


Use this to locate and select the chosen Array. The map window will switch to the map that contains the Array. This menu option is only available when you right-click on an entry in either [The Arrays Window](#) or the map window's Arrays list. It is not available from the map itself.



Figure 108. Array Management Drop-down Menu

Map Settings Window

This window provides tools that allow you to change the look of a map. You may change the label (name) that the map uses and the data displayed on information bars.

To change map properties, click the **Edit Map Settings** button  on the map toolbar, or right click the map in the **Maps** list and select **Properties** from the drop-down menu. The Edit Map Settings window has four separate pages which are accessible by making the proper selection from the tree on the left:

- **Map Settings**
- **Information Bars** (three pages: Array Data, Map Data, Location Data)

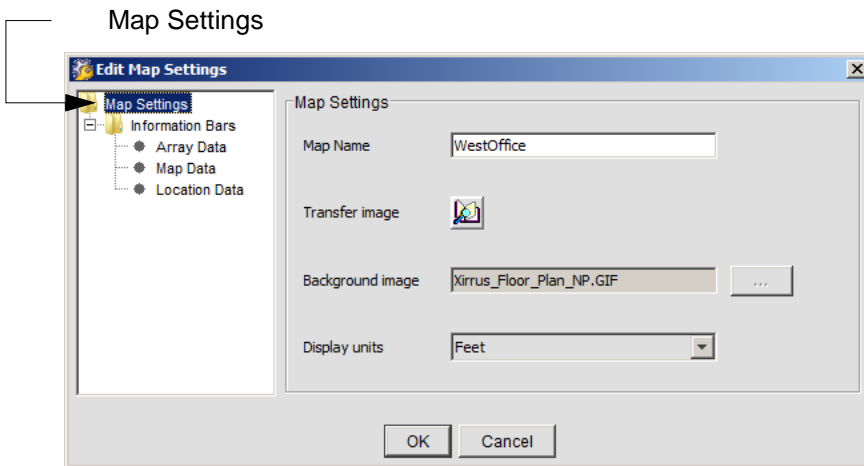


Figure 109. Map Settings Page

Map Settings

- **Map Name**
Specifies the label (name) of the map as it appears in the **Tree** and in the header bar of the map window.
- **Transfer Image**
Use this button to browse for the background image of your map and transfer the file to the proper location on the XMS server.

- **Background Image**

The Background Image cannot be modified.

- **Display Units**

Select the units of distance for the **Information Bars**, **Feet** or **Meters**.

Proceed to another settings page, or click **OK** if done.

Information Bars

This page of the Map Properties window allows you to select the fields that are present on the map information bars. Select one of these pages, then check the fields that you would like to have displayed. See **“Information Bars” on page 140** for more details.

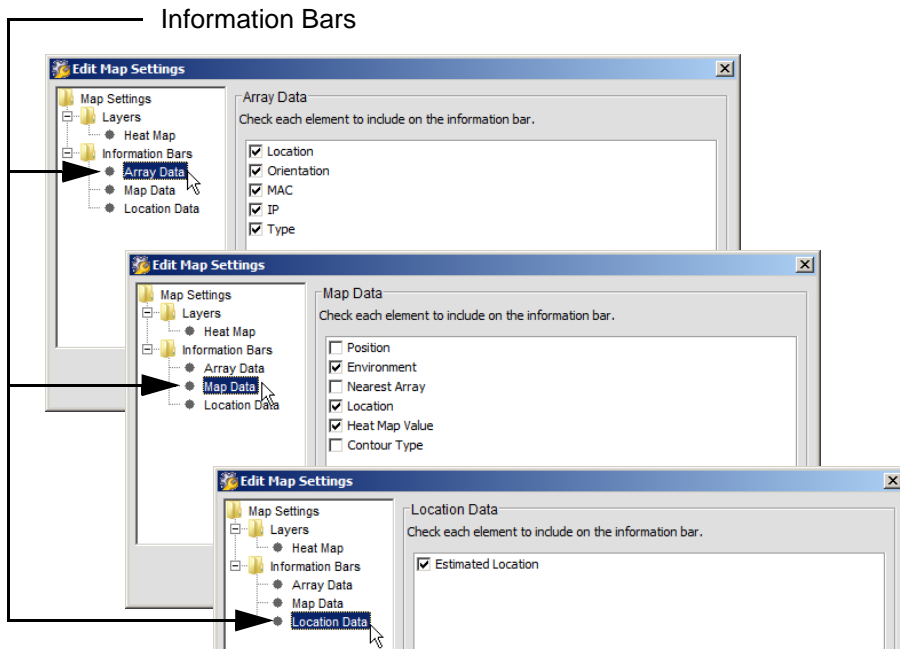


Figure 110. Map Settings - Information Bars

Proceed to another settings page, or click **OK** if done.



Managing Your Wi-Fi Arrays

This chapter provides instructions for using the Java client to manage your discovered Wi-Fi Arrays and Power over Gigabit Ethernet (PoGE) injectors, and includes managing wireless stations, individual IAPs (Integrated Access Points), and SSIDs. There is also a section discussing how to map PoGE injectors with the Arrays to which they supply power. Section headings for this chapter include:

- **“Arrays” on page 165**
- **“Managing Array Licenses” on page 189**
- **“IAPs” on page 198**
- **“Stations” on page 203**
- **“SSIDs” on page 207**
- **“PoGE Injectors” on page 211**

Choosing the Columns for Display

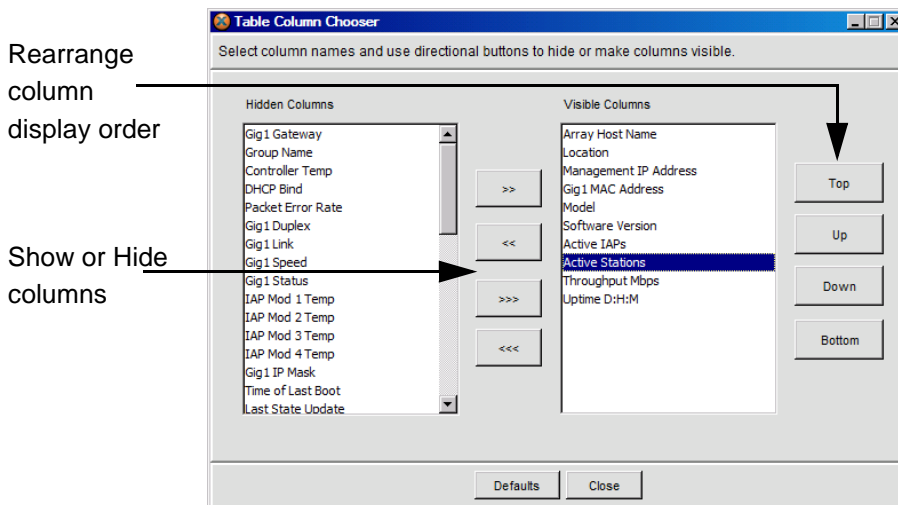



Figure 111. Table Column Chooser

The windows in the Resources section of the tree (except for Maps and SSIDs) may be customized by changing the columns that are displayed and the order of

display. If you prefer to use a smaller browser window for XMS and there's not enough room for all the columns to display, you can use this feature to select your preferred columns. Each of the windows has a Select Table Columns button  in the upper right corner. Click it to display the Table Column Chooser.

The **Visible Columns** list shows the columns that will be displayed. To hide a column, select it from the Visible Columns and click << to move it to the **Hidden Columns** list. Similarly, to display a column, select it from the Hidden Columns and click >> to move it to the Visible Columns list. There are also buttons to hide or display all columns (**Figure 111**). Use the **Top**, **Bottom**, **Up** and **Down** buttons to arrange the columns, left to right. Use the **Defaults** button to restore the columns that are displayed by default. Click **Close** when done.

Using the Search Feature in the Resource Windows

You may search for an Array using the **Find** function at the bottom left of **The Arrays Window**. You may search for an IAP or Station on their windows in the same way. The following rules apply to the search:

- The search is not case-sensitive.
- Entries containing the search string in any position in any displayed column are found. The target entries need not start with the search string.
- One entry at a time is found.
- As you type into the search field, the first entry that contains the search string is selected. As you type additional characters into the search field, the current entry remains highlighted as long as the entry contains the string. When the current entry ceases to match, the next entry in the list that matches the search string will be highlighted.
- If there are no matches to the current string, the **Find** field is displayed in red.
- To jump to the next matching entry, use the **Enter** key.

Arrays

This section provides instructions for configuring your Arrays, which includes assigning groups and policies, performing configuration, refreshing and rebooting an Array, viewing Array status, and viewing alarms and events. One especially useful feature allows you to create policies based on the configuration read directly from an Array.

The following topics are discussed:

- **"The Arrays Window" on page 166**
- **"Connecting to an Array" on page 172**
- **"Viewing Array Status" on page 172**
- **"Configuring an Array" on page 174**
- **"Create Policies from Array" on page 178**
- **"Enabling or Disabling IAPs" on page 180**
- **"Auto-Configuring Channels on Multiple Arrays" on page 181**
- **"Deleting an Array" on page 182**
- **"Removing an Array from a Map" on page 182**
- **"Assigning an Array to a Group" on page 183**
- **"Applying Policies to an Array" on page 185**
- **"Updating Array Software" on page 185**
- **"Viewing Events and Alerts" on page 186**
- **"Viewing Reports" on page 186**
- **"Refreshing an Array" on page 187**
- **"Rebooting an Array" on page 187**
- **"Locating an Array on a Map" on page 187**
- **"Managing a PoGE Injector" on page 187**



*Bulk Configuration is a powerful tool, available from the Tools option on the menu bar. This allows you to apply network or radio settings to a large number of Arrays at one time. To use this feature, please see **"Network Settings" on page 458** and **"Radio Settings" on page 466**.*

The Arrays Window

This window is displayed when you click on the **Arrays** node in the **Tree**, which appears under the Resources parent node. Information on this window is automatically refreshed every 20 seconds.

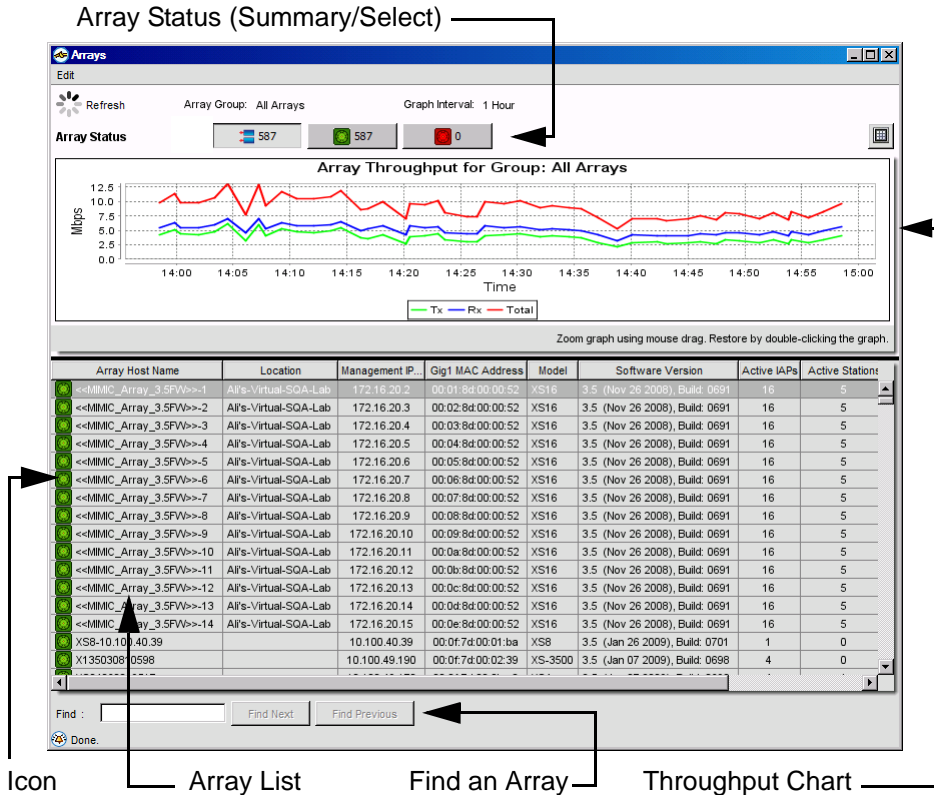


Figure 112. Arrays Window

The Arrays window is divided into three sections:

- **Array Status**—A count of Arrays by status; allows you to select the Arrays to be listed.
- **Array Throughput**—a chart of Array throughput.
- **Array List**—A list of Arrays, which allows you to perform a number of operations on a selected Array.

Array Status

The buttons at the top of the Arrays window summarize status information by showing the count of Arrays having each status value. The buttons also allow you to select the Arrays to be shown in the Array list based on status. (Figure 113) Hover the mouse over a button to display the status value represented by the button. You may click a button to filter the Array list, so that it shows only Arrays with the selected status.



Figure 113. Array Status Summary/Select Buttons

The following status buttons are shown:

- **Blue**—the **total** number of Arrays in the network. Click this button to show all Arrays in the Array list, regardless of status.
- **Green**—the number of Arrays that are **up**. Click this button to show only Arrays whose status is up in the Array list.
- **Red**—the number of Arrays that are **down**. An Array is considered to be down if XMS has been unable to communicate with it for over three minutes. Click this button to show only Arrays that are down in the Array list.

Array Throughput

The line graphs in this chart display aggregate data throughput for the same group of Arrays and time period that is selected in the Dashboard.

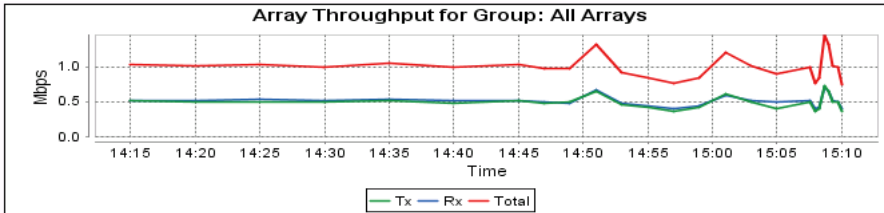


Figure 114. All Array Throughput

This chart is very similar to the Performance chart in the Dashboard (see [“Performance” on page 98](#)). If a group is selected in the Dashboard, then this chart shows data for that same group; otherwise, data for all Arrays is shown. Transmit throughput is shown in green, receive throughput is shown in blue, and total throughput is shown in red. The chart shows data for the last hour by default, but if you change the Interval displayed on the Dashboard, this chart will show the same interval.

You may zoom in on an area of the graph by selecting the area of interest with the mouse. Click and drag to select a region. When you release the mouse button, the chart will show the selected region. Double-click anywhere in the chart to revert to showing the entire chart. You may resize the chart by dragging the border between it and the Array list. It may be reduced to the point where it disappears. To make it visible again, drag the border down until the chart has the desired height.

Array List

Array Host Name	Location	Management IP	Gig1 MAC Address	Model	Software Version	Active IAPs	Active Stations	Throughp
<<MMMC_Array_3.5FW>>-1	All's-Virtual-SQA-Lab	172.16.20.2	00:01:8d:00:00:52	XS16	3.5 (Nov 26 2008), Build: 0691	16	5	0.007
<<MMMC_Array_3.5FW>>-2	All's-Virtual-SQA-Lab	172.16.20.3	00:02:8d:00:00:52	XS16	3.5 (Nov 26 2008), Build: 0691	16	5	0.007
<<MMMC_Array_3.5FW>>-3	All's-Virtual-SQA-Lab	172.16.20.4	00:03:8d:00:00:52	XS16	3.5 (Nov 26 2008), Build: 0691	16	5	0.007
<<MMMC_Array_3.5FW>>-4	All's-Virtual-SQA-Lab	172.16.20.5	00:04:8d:00:00:52	XS16	3.5 (Nov 26 2008), Build: 0691	16	5	0.007
<<MMMC_Array_3.5FW>>-5	All's-Virtual-SQA-Lab	172.16.20.6	00:05:8d:00:00:52	XS16	3.5 (Nov 26 2008), Build: 0691	16	5	0.007
<<MMMC_Array_3.5FW>>-6	All's-Virtual-SQA-Lab	172.16.20.7	00:06:8d:00:00:52	XS16	3.5 (Nov 26 2008), Build: 0691	16	5	0.007
<<MMMC_Array_3.5FW>>-7	All's-Virtual-SQA-Lab	172.16.20.8	00:07:8d:00:00:52	XS16	3.5 (Nov 26 2008), Build: 0691	16	5	0.007
<<MMMC_Array_3.5FW>>-8	All's-Virtual-SQA-Lab	172.16.20.9	00:08:8d:00:00:52	XS16	3.5 (Nov 26 2008), Build: 0691	16	5	0.007
<<MMMC_Array_3.5FW>>-9	All's-Virtual-SQA-Lab	172.16.20.10	00:09:8d:00:00:52	XS16	3.5 (Nov 26 2008), Build: 0691	16	5	0.007
<<MMMC_Array_3.5FW>>-10	All's-Virtual-SQA-Lab	172.16.20.11	00:0a:8d:00:00:52	XS16	3.5 (Nov 26 2008), Build: 0691	16	5	0.007
<<MMMC_Array_3.5FW>>-11	All's-Virtual-SQA-Lab	172.16.20.12	00:0b:8d:00:00:52	XS16	3.5 (Nov 26 2008), Build: 0691	16	5	0.007
<<MMMC_Array_3.5FW>>-12	All's-Virtual-SQA-Lab	172.16.20.13	00:0c:8d:00:00:52	XS16	3.5 (Nov 26 2008), Build: 0691	16	5	0.007
<<MMMC_Array_3.5FW>>-13	All's-Virtual-SQA-Lab	172.16.20.14	00:0d:8d:00:00:52	XS16	3.5 (Nov 26 2008), Build: 0691	16	5	0.007
<<MMMC_Array_3.5FW>>-14	All's-Virtual-SQA-Lab	172.16.20.15	00:0e:8d:00:00:52	XS16	3.5 (Nov 26 2008), Build: 0691	16	5	0.007
XSS-10.100.40.39		10.100.40.39	00:0f:7d:00:01:ba	XS8	3.5 (Jan 26 2009), Build: 0701	1	0	0.075
X135030810598		10.100.49.190	00:0f:7d:00:02:39	XS-3500	3.5 (Jan 07 2009), Build: 0698	4	0	0.029

Find : Find Next Find Previous

Done.

Figure 115. Array List

This list shows Arrays connected to the network. Use the **Array Status** buttons to select which Arrays to display—all Arrays, or only those with the selected status. Only Arrays that belong to the group selected on the Dashboard window are displayed. To search for a particular Array, see [“Using the Search Feature in the Resource Windows” on page 164](#).

You may customize the columns shown in this list—see [“Choosing the Columns for Display” on page 163](#). For each Array, the following information is shown by default:

- The icons to the left of the first column in the list are color-coded to denote the current status of each Array. For example, if an icon shows that the Array is clear then it is highlighted in GREEN. If the icon shows that the Array has a critical problem then RED is used.
- The **Array Host Name**
- The **Location** of the Array
- The **Management IP Address** of the Array
- The **Gig1 MAC Address** of the Array (MAC address of the Gigabit1 port)
- The **Model** of the Array
- The **Software Version** currently running on the Array

- The number of **Active IAPs** on the Array.
- The number of **Active Stations** associated to this Array
- The current **Throughput** Mbps of the Array
- The current **Uptime** of this Array (since the last reboot)



An Array's Host Name will typically be used to identify the Array throughout the XMS user interface. In places where a specific attribute such as IP address is called out, then that value will be shown.

Array Operations

There are a number of Array operations that can be performed from XMS. Before we discuss the specifics, you should be aware that there are two methods for accessing Array configuration menus. (Figure 116) These include:

- **Method 1:** Select the **Arrays** node in the **Tree**, then right-click on an Array in the table to generate a pull-down list of menu items.
- **Method 2:** Select an Array icon in a map, then right-click on the Array to generate a pull-down list of menu items. The list of menu items is the same as the list you generate with the second method.

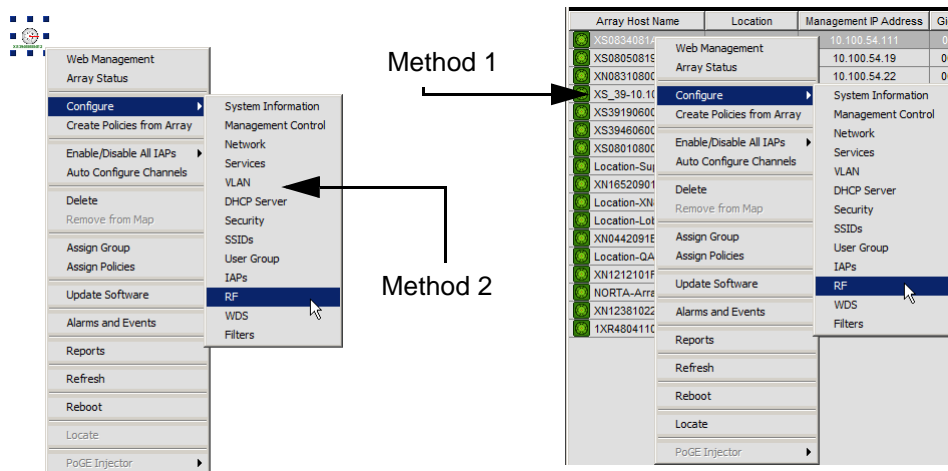


Figure 116. Menu Items for Configuring Arrays

To avoid duplication and to maintain consistency, we assume that you will use method 1 (the Arrays window) to access an Array's configuration menu items—from the **Arrays** node in the **Tree**. You may select multiple Arrays from the list. The chosen operation will be applied to all selected entries, if appropriate.

The following operations are available when you select and then right-click on an Array in the list:

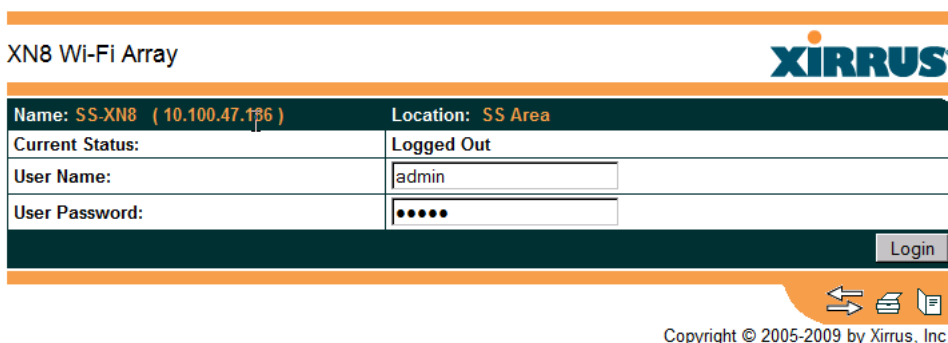
- [“Connecting to an Array” on page 172](#)
- [“Viewing Array Status” on page 172](#)
- [“Configuring an Array” on page 174](#)
- [“Create Policies from Array” on page 178](#)
- [“Enabling or Disabling IAPs” on page 180](#)
- [“Auto-Configuring Channels on Multiple Arrays” on page 181](#)
- [“Deleting an Array” on page 182](#)
- [“Removing an Array from a Map” on page 182](#)
- [“Assigning an Array to a Group” on page 183](#)
- [“Applying Policies to an Array” on page 185](#)
- [“Updating Array Software” on page 185](#)
- [“Viewing Events and Alerts” on page 186](#)
- [“Viewing Reports” on page 186](#)
- [“Refreshing an Array” on page 187](#)
- [“Rebooting an Array” on page 187](#)
- [“Locating an Array on a Map” on page 187](#)
- [“Managing a PoGE Injector” on page 187](#)

Sorting the List of Arrays

To change how the table is sorted, click in any column header to define that header as the sort criteria. In addition, you can choose to have the results displayed in ascending or descending order, represented by the appropriate arrow icon. To do this, simply click in the same header again to toggle between ascending and descending order.

Connecting to an Array

To connect to an Array, select and then right-click the Array in the Java client Arrays window, then choose **Web Management** from the pull-down list. The Array's Web Management Interface login window is displayed as a separate browser window (not part of the XMS client interface). From here you can log in to the Array with your user name and password (the default for both is **admin**). Note that the XMS server will attempt to connect to the Array using the **HTTPS Port** specified in the Management Control policy.



Name: SS-XN8 (10.100.47.196)		Location: SS Area	
Current Status:	Logged Out		
User Name:	admin		
User Password:	•••••		
Login			

Copyright © 2005-2009 by Xirrus, Inc.

Figure 117. Array Login Window

After logging in to the Array, if you make any configuration changes, they will not be propagated to all Arrays in the network. When managing multiple Arrays with XMS, you should make configuration changes from XMS's client interface.

For detailed information about configuring an Array, refer to the *Wi-Fi Array User's Guide*, part number 800-0006-001.

Viewing Array Status

To view a summary of information for a selected Array and its components, right-click on the Array and choose **Array Status** from the pull-down list. The Array Status window is displayed.

management settings (whether the port is enabled and whether management of the Array is allowed via this port).

- Wireless Interfaces - lists the IAPs present on this Array, as well as channel, cell size, active stations, and whether the IAP is enabled. For more information about IAPs, see [“IAPs” on page 198](#).
- Management Access - whether access via SSH and/or Telnet is enabled.

Configuring an Array

You can configure a specific Array or you can create configuration policies and apply these policies to an Array, multiple Arrays, or groups of Arrays. If you want to configure a specific Array, select and then right-click on the Array and choose **Configure** from the pull-down list—this generates a new pull-down list with all available configuration options. ([Figure 119](#))

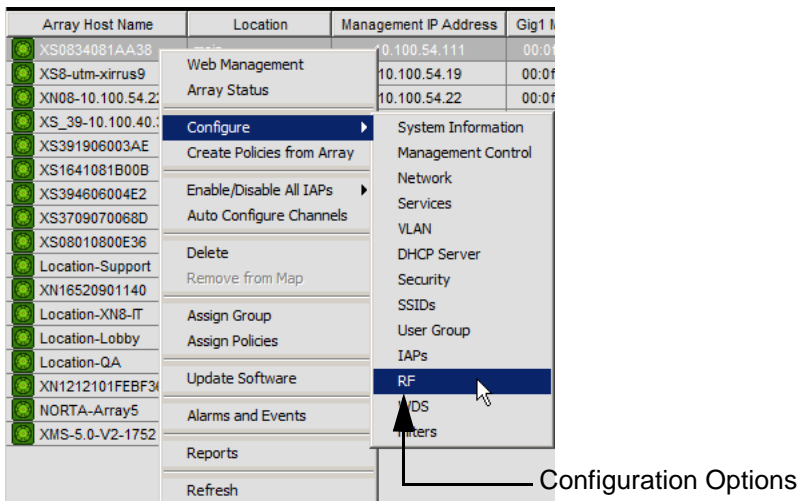


Figure 119. Configuring an Array

The configuration options for a selected Array are similar to the configuration options presented to you when creating configuration policies. To avoid repetition, refer to the [“List of Configuration Policies” on page 177](#) when making configuration changes to a specific Array.

When you choose to configure a specific option, the configuration window for the selected option is displayed. The main differences between this window and the corresponding policy creation window are the inclusion of an **Execute** button, and the fact that this window shows the currently configured values on the Array.

Occasionally the fields shown in this window may differ slightly from those in the policy window. For example, when configuring **System Information** on an Array, fields for **Host Name** and **Location** are shown. These fields are absent from the policy window ([Figure 158 on page 226](#)) since it would be incorrect to set the same host name and location for multiple Arrays. Duplicating the host name would actually cause serious problems.

After making configuration changes at the Array level, you must click on the **Execute** button to apply your changes. ([Figure 120](#))

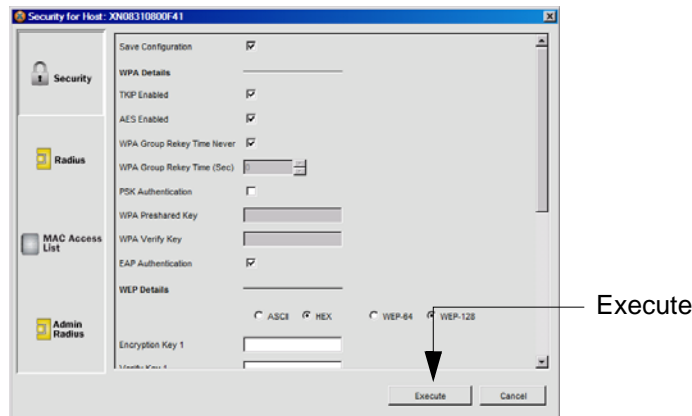


Figure 120. Configuring an Array

Executing the Configuration Change

After a successful execution of the command, the Task Results window is displayed, which confirms the changes you made. You can choose to have the results displayed as a table, as plain text, or in HTML format—the default is to have the results displayed in tabular (table) form.

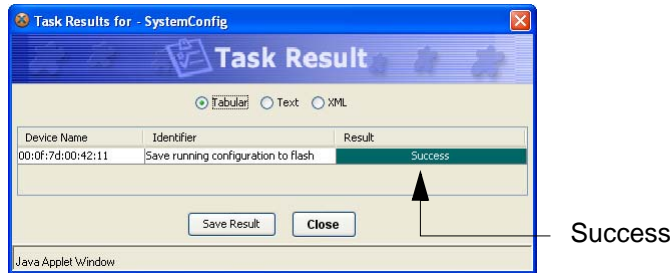


Figure 121. Task Results (success)

Saving Results

If you would like to save the results of your configuration changes, click on the **Save Result** button. In this case, you are prompted to enter a file name for the saved results file. Enter the file name, then click on the **OK** button.



Figure 122. Save Results

What if the Configuration Changes are Rejected?

If the configuration changes you make are not implemented successfully after clicking on the **Execute** button, the Task Results window indicates that the command failed.

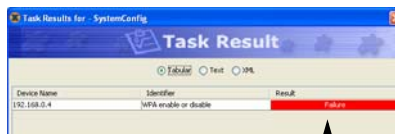


Figure 123. Task Results (Failure)

List of Configuration Policies

The following list of configuration policies is provided as a reference that corresponds to the menu of configuration options in the pull-down list.

- **System Information**
- **Management Control**
- **Network**
- **Services**
- **VLAN**
- **DHCP Server**
- **Security**
- **SSIDs**
- **User Groups**
- **IAPs**
- **RF**
- **WDS**
- **Filters**

Create Policies from Array

This powerful feature allows you to use the configuration of any Array in the network as a pattern for creating XMS policies. Let's say you've already configured an Array and you'd like to set up other Arrays the same way. Simply select the model Array in the Array Window, right-click on it, and use the **Create Policies from Array** feature to select the types of policies to create based on the model. (Figure 124) You can then apply these new policies to other Arrays to set their configuration to be the same as the model Array.

When you use **Create Policies from Array**, a dialog box allows you to select the policies that you wish to create.

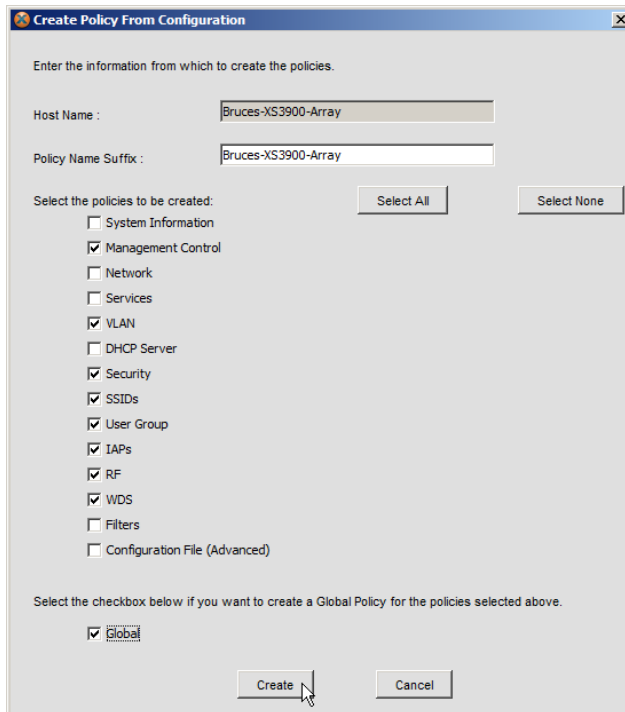


Figure 124. Create Policies from Array

Host Name shows the Host Name, IP address, or MAC address of the selected Array. **Policy Name Suffix** determines the names of the newly created policies—the new policy is normally named <type-HostName>. For example, in

Figure 124, the VLAN policy that is created using the configuration pulled from the Array will be named **vlan-SSArray**. You may edit the **Policy Name Suffix** used to create the names for the new policies. Note that you may create policies from a number of Arrays—the resulting policies will all have unique names.

Use the checkboxes to select each of the policy types that you wish to create. Check the **Global** checkbox if you also wish to create a **Global Policy** based on this Array. The global policy will include all of the policies that you selected. If you apply this global policy to an Array, then all of the configuration that you read from the model Array will be applied in one step. The global policy is a handy shortcut, rather than applying each of the created policies individually.

Click the **Create** button when you have selected the types of policies to be created. XMS will list the policies to be created along with their names. (**Figure 125A**)

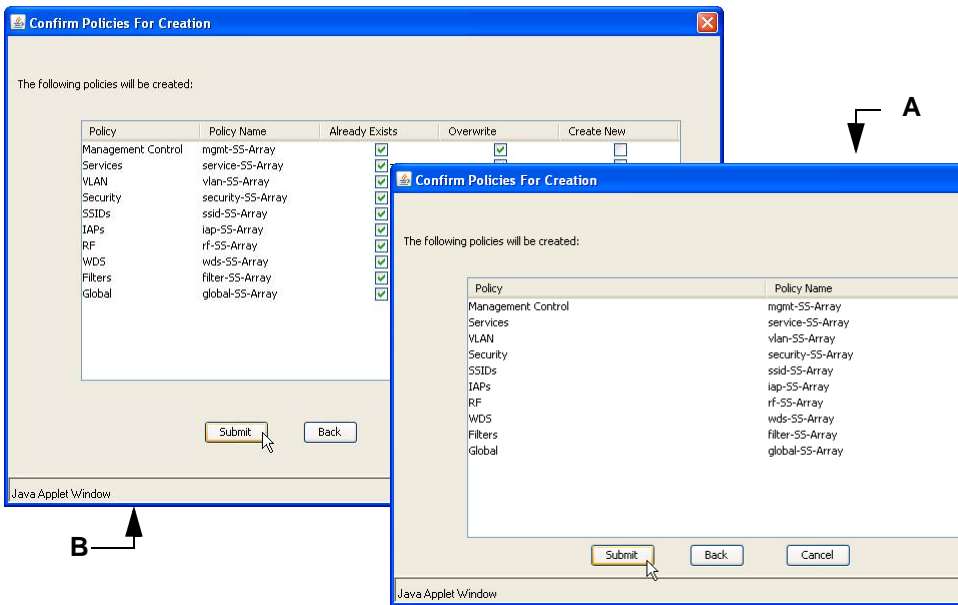
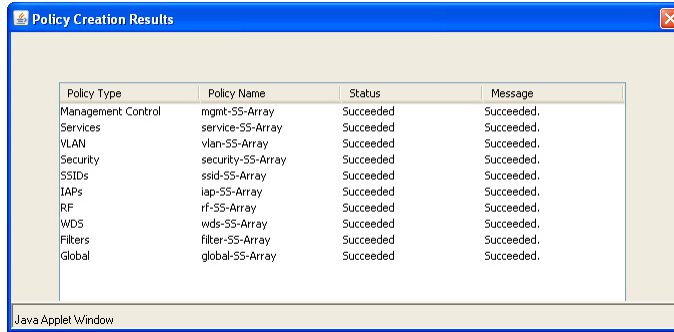


Figure 125. Confirm Policies to be Created (First and Subsequent times)

If you have previously created policies from this Array, XMS will list the policies that you’ve requested and classify them as **Already Exists** or **Create New** (**Figure 125B**). For pre-existing policies, the **Overwrite** column is checked. This

means that the new policy will overwrite the previous policy. If you clear the checkbox, XMS will keep the old policy and create a new one with a new name. XMS appends **-1**, **-2**, etc., to create the new policy name. Click the **Submit** button to proceed. The results of the operation will be displayed.



Policy Type	Policy Name	Status	Message
Management Control	mgmt-SS-Array	Succeeded	Succeeded.
Services	service-SS-Array	Succeeded	Succeeded.
VLAN	vlan-SS-Array	Succeeded	Succeeded.
Security	security-SS-Array	Succeeded	Succeeded.
SSIDs	ssid-SS-Array	Succeeded	Succeeded.
IAPs	iap-SS-Array	Succeeded	Succeeded.
RF	rf-SS-Array	Succeeded	Succeeded.
WDS	wds-SS-Array	Succeeded	Succeeded.
Filters	filter-SS-Array	Succeeded	Succeeded.
Global	global-SS-Array	Succeeded	Succeeded.

Java Applet Window

Figure 126. Results of Create Policies from Array

For more information on using policies, please see [“Managing Configuration with Policies” on page 215](#).

Enabling or Disabling IAPs

This option allows you to quickly disable all of the IAPs on one or more Arrays, and later re-enable them. For example, a school district might use this to disable all wireless access at night.

To disable IAPs, first select one or more Arrays whose IAPs are to be disabled. You may use **Ctrl+Click** to add Arrays one at a time, **Shift+Click** to select a range of entries, or **Ctrl+A** to select the entire list. Next right-click anywhere in the Array list portion of the Arrays window and select **Enable/Disable All IAPs** from the right-click menu. Select **Disable**. You will be asked to confirm that you wish to change the status of all IAPs on the selected Arrays. Click **Yes** to proceed.

To enable IAPs, again select the desired Arrays. Select **Enable/Disable All IAPs > Enable** from the right-click menu, and click **Yes** to confirm the operation.

Auto-Configuring Channels on Multiple Arrays

Auto Channel assignment is the preferred way to select channel assignments for an Array's IAPs, and has significant advantages. When you start an Array's auto channel feature, the Array scans the surrounding area for RF activity on all channels and then automatically selects and sets its channels to the best available. This function is typically executed when initially installing Arrays in a new location. You may wish to repeat it periodically to account for changes in the RF environment over time.

When running auto channel on multiple Arrays, XMS will shut down IAPs on all of the Arrays being configured. It will then run auto channel on one Array at a time, and bring its radios back up when channels have been selected.

First select one or more Arrays whose channels are to be auto-configured. You may use **Ctrl+Click** to add Arrays one at a time, **Shift+Click** to select a range of entries, or **Ctrl+A** to select the entire list. Next right-click anywhere in the Array list portion of the Arrays window and select **Auto Configure Channels** from the right-click menu. You will be asked to confirm that you wish to run auto-configuration. Click **Yes** to proceed.

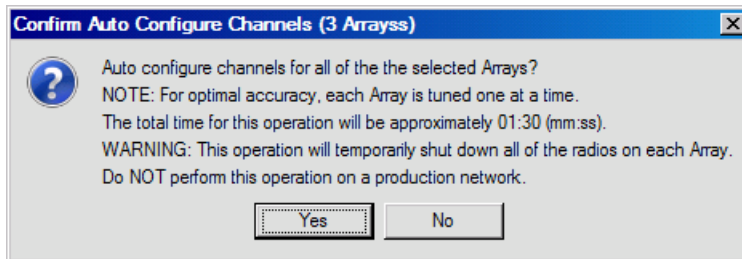


Figure 127. Auto Configure Confirmation Dialog

Auto-configure typically takes about 30 seconds per Array.

Deleting an Array

To delete an Array from the list of managed Arrays, select and then right-click on the Array and choose **Delete** from the pull-down list. When prompted, click on the **Yes** button to delete the Array, or click on the **No** button to abort the request.

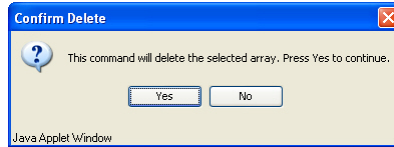


Figure 128. Deleting an Array

If you delete an Array, you can always re-discover the Array or manually add it to the list of managed Arrays. To do this, go to **“Adding an Array or PoGE Injector” on page 87**.

Removing an Array from a Map

If this Array is assigned to a map, then you may use this option to remove the Array from the map. See **“Adding Arrays to Maps” on page 147**. This does not delete an Array from the list of managed Arrays.

Assigning an Array to a Group

To assign one or more Arrays to a group, select the Array(s) and then right-click and choose **Assign Group** from the pull-down list. The Assign Array(s) to Group(s) window is displayed. (Figure 129)

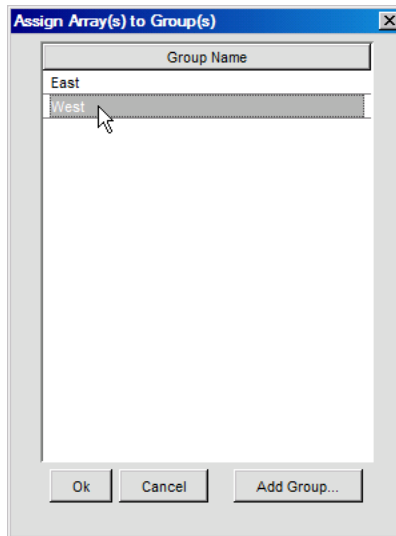


Figure 129. Assigning a Group

Before you can add Arrays to an Array group, the group must exist. You may create groups in advance using a Group policy (see [“Creating A New Group” on page 366](#)), or you may create groups directly from the Assign Arrays window as described below.

To create a new Array group, click the **Add Group** button on the lower left. Enter a name for the new group in the resulting dialog box and click **OK**. Changes made here will be reflected in the **Groups** policies as well and vice versa.

The Arrays Window, Group Policies, and the Dashboard

Any changes made here will appear in the **Groups** policies as well, and vice versa. Changes made in either place will also be reflected almost immediately on the Dashboard. Recall that you may select a particular Array group to display in the Dashboard (using the **Array Group** field on the upper right of the Dashboard

window). The Dashboard will filter data to display only data for the selected group (and certain other windows, such as Arrays and IAPs, will also show filtered results). For instance, if you have selected an Array group on the Dashboard and you have added Arrays to that group, those Arrays will be included in the data shown on the Dashboard.

More Information About Groups

The following list is provided as a reference when managing Array groups:

- [“Groups” on page 366](#)
- [“About Dashboard Data” on page 92](#)
- [“Creating a Map Group” on page 196](#)
- [“Unassigning Groups” on page 195](#)

Applying Policies to an Array

Use this option to apply policies to an Array and change its configuration. Before you can apply a policy to an Array, the policy must exist. To create a new policy, go to **“Managing Configuration with Policies” on page 215**. To apply a policy (or policies) to the Array, select and then right-click the Array and choose **Assign Policies** from the pull-down list. The Global Policy window is displayed.

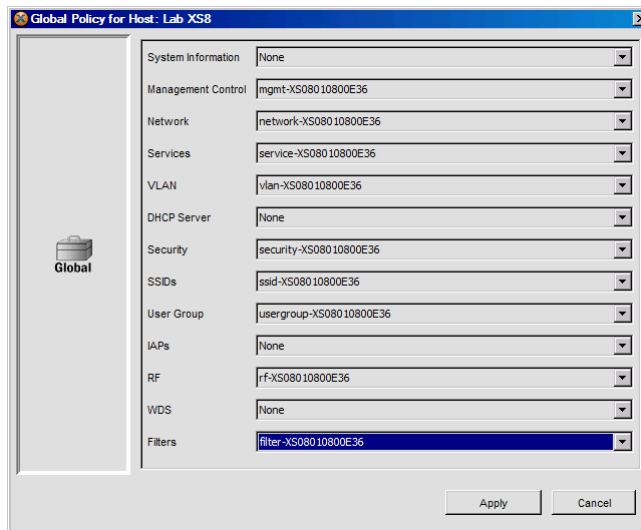


Figure 130. Assigning Policies

Choose the policy (or policies) you want to apply from the pull-down lists associated with each category, then click on the **Apply** button to apply the chosen policies to the Array, or click on the **Cancel** button to abort the request. In each category, select None if you wish to make no changes to that category of configuration on the Array, i.e., to leave it as-is.

Updating Array Software

You may use the right-click menu to apply an existing Software Update policy to an Array (see **“Software Update” on page 354** for more about creating these policies). Right-click the Array and choose **Update Software** from the pull-down list. Select the desired policy from the Software Update Policy window.

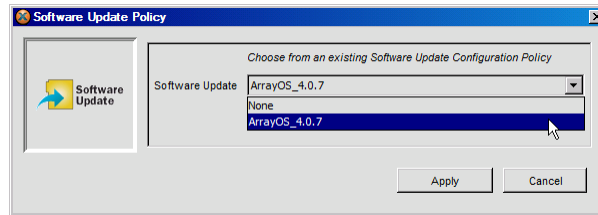


Figure 131. Updating Array Software Image

When prompted, click on the **Yes** button to update the selected Array, or click on the **No** button to abort the request.

Viewing Events and Alerts

To view a tabular summary of events and alerts for a selected Array, right-click on the Array and choose **Alarms and Events** from the pull-down list. The Events and Alerts summary window is displayed, with the displayed results specific to the selected Array. For more information about Events and Alerts, go to **“Monitoring Your Network” on page 105**.

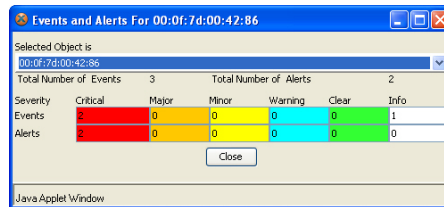


Figure 132. Viewing Events and Alerts

Viewing Reports

To access the Reports window, right-click an Array and choose **Reports** from the pull-down list. For more information about reports, see **“Managing Reports” on page 371**.

Refreshing an Array

When you refresh an Array, XMS polls the Array and verifies that the Array is still reachable by the system. To refresh an Array, select and then right-click the Array and choose **Refresh Array** from the pull-down list. For more information about refreshing an Array, go to [“Refreshing a Device” on page 88](#).

If the refresh process fails it may be necessary to [delete the Array](#) from the list then exit and restart the XMS client and allow XMS’s discovery feature to discover the Array, or reboot the Array so that it will announce itself to XMS using the [Phone Home](#) feature.

Rebooting an Array

To reboot an Array, select and then right-click on the Array and choose **Reboot Array** from the pull-down list. When prompted, click on the **Yes** button to reboot the selected Array, or click on the **No** button to abort the request.

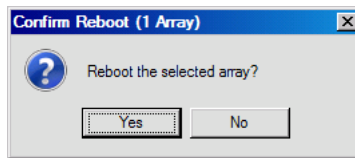


Figure 133. Rebooting an Array


Be patient while the Array reboots. The reboot process may take several minutes.

Locating an Array on a Map

If this Array is assigned to a map, then you may use this option to display that map. See [“Adding Arrays to Maps” on page 147](#).

Managing a PoGE Injector

From the Array window, you may view the status of PoGE output ports that have been mapped to Arrays (see [“Associate the Injector with an Array” on page 212](#)). You may also turn injector output ports on or off.

To display the PoGE Status column in the Arrays list, click the **Column Selector** button  located at the upper right of the Array Throughput graph. **PoGE Status** displays the status of injector ports connected to an Array:

- **On**—all mapped PoGE ports are supplying nominal power to the Array.
- **Off**—all mapped PoGE ports are off.
- **Fault**—if a problem is detected on a PoGE port, the type of problem is indicated.
- **NA**—no PoGE ports are associated with the Array (see [page 212](#)).
- **blank**—Array model does not support PoGE.

You may turn a PoGE injector output port on or off, thus turning power on or off to the connected Array port. Right-click the desired Array. Select **PoGE Injector** from the drop-down menu. The following options are displayed:

- **Power On** - turn on power and data transmission on the injector port(s), thus supplying power and data to the connected Array port(s). If the injector port(s) are already on, transmission will not be affected.
- **Power Off** - turn off power and data transmission on the injector port(s). The connected Array port(s) will not be powered. If the injector port(s) are already off, they will not be affected.
- **Power Cycle** - turn all connected injector ports off and then on again. This reboots the Array.

Select one of the above operations. You will be asked to verify that you wish to proceed. The status of the operation will be displayed.

Managing Array Licenses

XMS includes a browser-based utility that manages the licenses for large numbers of Arrays. You can easily view licensing information for your Arrays and manage individual licenses. The license utility can apply bulk licenses in one step, by simply reading in the .csv license file issued by Xirrus. Similarly, when it's time to upgrade all of your Arrays with new features or a major software release, the required licenses may all be installed in one step.



This section describes using XMS to manage Array licenses. If you are looking for information regarding the XMS server's license, please see "Licensing the XMS Server" on page 35.

About Licensing and Upgrades

An Array's license determines many of the features that are available on the Array. For example, automatic cell sizing and channel allocation require a license that includes the Xirrus Advanced RF Performance Manager (RPM). Also, IEEE 802.11n operation on XN model Arrays is a licensed feature. To check the features supported by your license, see the next section—**The Array Licensing Window**. For more information on the features that require a license, please see "**Advanced Feature Sets**" in the **Introduction** chapter of the *Xirrus Wi-Fi Arrays User's Guide*.

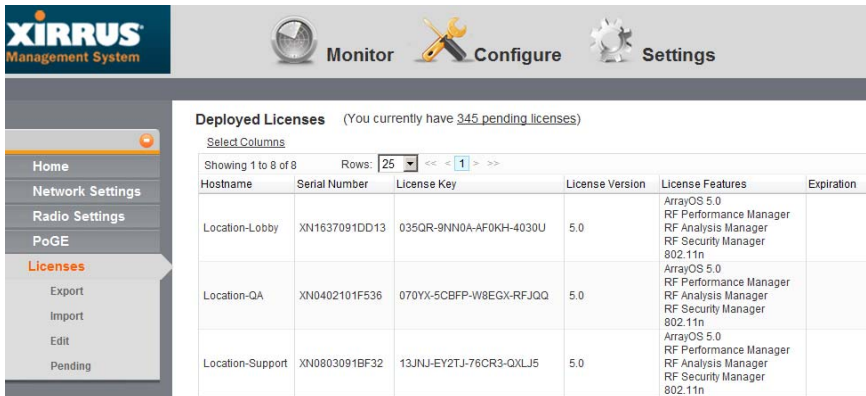
If you are upgrading an Array to add new features that are not supported by your existing license, **you must enter the new license key that includes the upgrade's features before upgrading.**

Similarly, if you are upgrading an Array for a new software release, **you must enter the new license key that enables the operation of that release before upgrading.** Major releases will need a new license key, but minor releases will not. For example, to upgrade from ArrayOS Release 5.0.5 to Release 5.1, you must enter a new license. To upgrade from ArrayOS Release 5.0.5 to Release 5.0.8, use the existing license.

The Array Licensing Window

This window is displayed by your browser when you select **Tools > Array License Management** from the **Menu Bar** on top of **The XMS Java Client Interface**. (You may also access this page using the web client, by clicking **Configure** on the top of the window, and then selecting the **Licenses** page. See “**About Configure Pages**” on page 425.)

Initially, this page displays a list of all *deployed* Array licenses being managed by XMS. This is a list of all discovered Arrays and their licenses. By default the following is shown for each Array: the **License Key**, the **Hostname** along with the Array **Serial Number**, the **License Version** and **Features** supported by the license, and the license **Expiration** date. You may use the **Select Columns** option to choose which information you wish to display.



Hostname	Serial Number	License Key	License Version	License Features	Expiration
Location-Lobby	XN1637091DD13	035QR-9NN0A-AF0KH-4030U	5.0	ArrayOS 5.0 RF Performance Manager RF Analysis Manager RF Security Manager 802.11n	
Location-QA	XN0402101F536	070YX-5CBFP-W8EGX-RFJQQ	5.0	ArrayOS 5.0 RF Performance Manager RF Analysis Manager RF Security Manager 802.11n	
Location-Support	XN0803091BF32	13JNJ-EY2TJ-76CR3-QXLJ5	5.0	ArrayOS 5.0 RF Performance Manager RF Analysis Manager RF Security Manager 802.11n	

Figure 134. Array License Management - Deployed Licenses

The **Features** column shows the advanced features that are enabled by this license, such as the RF Performance Manager (RPM), RF Security Manager (RSM), RF Analysis Manager (RAM), or IEEE 802.11n operation.

The following main operations are available for managing licenses:

- Viewing deployed licenses on discovered Arrays, described above.
- **Exporting Array Licenses**
- **Importing Array Licenses**

- **Editing Array Licenses**
- **Managing Pending Array Licenses**



*If you change a license directly using the CLI or WMI on an Array whose license status is **Deployed**, XMS will detect the change and display the changed license in the list of deployed licenses.*

However, if XMS has a license pending for that Array, that license will be deployed as soon as XMS is able to do so, replacing the license in the Array.

Exporting Array Licenses

At times, you may wish to export Array licenses to a file. For example, you may want a consolidated record of some or all of your licenses, or Xirrus Customer Service may request this information to resolve a support issue. This feature exports the selected licenses shown on the Deployed Licenses window into a file that can be imported by Excel—either a .csv file or an .xls file. This file may also be used for **Importing Array Licenses**. To export Pending licenses, see “Managing Pending Array Licenses” on page 196.

1

Select Arrays

2

Download Licenses

< Previous

Next >

Select the arrays for which you wish to export licenses and click Next.

Select Columns

Showing 1 to 8 of 8

Rows: 25

<< 1 >>

<input type="checkbox"/>	Status	Hostname	IP Address	Location	Model	Stations	Software Version	Gig1 Mac Address	Uptime
<input checked="" type="checkbox"/>		Location-Lobby	10.100.46.239	test	XN16	0	5.0.0 (Oct 06 2010), Build: 1531	00:0f7d:00:d2:a2	1 da
<input checked="" type="checkbox"/>		Location-QA	10.100.46.237	test	XN4	0	5.0.0 (Oct 06 2010), Build: 1531	00:0f7d:01:1e:4c	30 d
<input checked="" type="checkbox"/>		Location-Support	10.100.46.240	test	XN8	1	5.0.0 (Oct 06 2010), Build: 1531	00:0f7d:00:76:48	1 da
<input checked="" type="checkbox"/>		Location-XN8-IT	10.100.46.238	test	XN8	0	5.0.0 (Oct 06 2010), Build: 1531	00:0f7d:00:c3:bd	1 da
<input type="checkbox"/>		showNetsXN8-14	10.105.4.102		XN8	75	5.0.1 (Nov 10 2010), Build: 1535	00:0f7d:01:1c:85	0 da

Figure 135. Exporting Array Licenses

To export deployed licenses, first display the Array License Management window in your browser by selecting **Tools > Array License Management** from the **Menu**

Bar on top of **The XMS Java Client Interface**. Click the **Licenses** link on the left, and then click the **Export** link that appears underneath to display all deployed licenses. (**Figure 135**)

To proceed, select the desired licenses by checking them off in the first column. Click the **Next >** button at the top of the page.

To export an .xls file, click the **Excel** radio button. To export a file of comma-separated values (.csv), click the **Csv** radio button. Then click **Export**. The File Download dialog box will allow you to open the file, or save it to the location you select.

	A	B	C	D	E	F	G	H	I
1	Hostname	Serial Number	License Key	License V	Feature0	Feature1	Feature2	Feature3	Feature4
2	Location-Lobby	XN1637091DD13	035QR-9NN0A-AF0KH-4030U	5	802.11n	RAM	RPM	RSM	
3	Location-QA	XN0402101F536	070YX-5CBFP-W8EGX-RFJQQ	5	802.11n	RAM	RPM	RSM	
4	Location-Support	XN0803091BF32	13JNJ-EY2TJ-76CR3-QXLJ5	5	802.11n	RAM	RPM	RSM	
5	Location-XN8-IT	XN0834091D82F	1ETGD-0YKFW-0YWT7-23AAY	5	802.11n	RAM	RPM	RSM	

Figure 136. Sample Export File

This exports the selected deployed licenses into a file of the selected format. A sample export file is shown in **Figure 136**.

Importing Array Licenses

Use this feature to import a .csv or .xls file with licensing information for any number of Arrays. For example, to upgrade your entire Xirrus Wi-Fi network to a new major software release, you must first deploy licenses for that release. Xirrus will furnish these licenses to you in the form of an Excel (.csv) file. Simply click to import the file and click **Finish** to deploy the licenses to the appropriate Arrays.

After your license file has been imported, any licenses that are for XMS managed Arrays (i.e., those that have been discovered) will be deployed to those Arrays. The Array is not rebooted but the radios will go down and up, so that station associations will be disrupted briefly. The Array will start using the new license, and will support the capabilities shown in the **Features** column.

A license for an Array that is not yet under XMS management will be deployed as soon as the target Array is discovered. Similarly, a license for a managed Array that is down will be deployed shortly after it comes back on line.

To import licenses, first display the Array License Management window in your browser by selecting **Tools > Array License Management** from the **Menu Bar** on top of **The XMS Java Client Interface**. Click the **Licenses** link on the left, and then click the **Import** link that appears underneath it. Fields are displayed to allow you to specify the license file.

.Click the **Choose file** button to select the license file. It must be either an .xls or a .csv (comma-separated values) file. To see an example of the format, you may export a sample license file (see **“Exporting Array Licenses” on page 191**). The File Download dialog box will allow you to open the file, or save it to the location you select. Click the **Upload** button. When the upload is complete, click **Next >** at the top of the page.

The imported licenses will be displayed on the Verify Licenses page. (**Figure 137**) Check that the licenses imported correctly. If necessary, you may edit any **License Key** by clicking on it.

Verify your licenses imported correctly then click Finish to complete the import process. Any licenses that cannot be deployed now either because the array has not yet been discovered by XMS or because the array is off line will be placed in the pending list and will be deployed when the array is available.

Select Columns

Showing 1 to 8 of 8 Rows: 25 << 1 >>

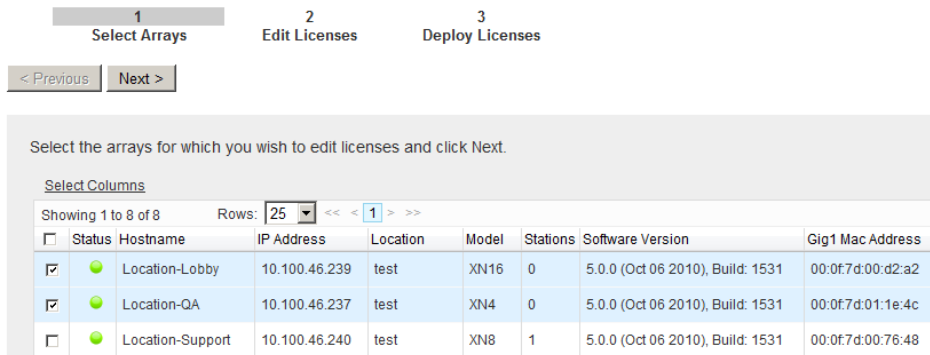
License Key	Serial Number	License Status	Software Version	Features
035QR-9NN0A-AF0KH-4030U	XN1637091DD13	Array Not Discovered		802.11n RF Analysis Manager RF Performance Manager RF Security Manager
070YX-5CBFP-W8EGX-RF-10Q	XN0402101F536	Array Not Discovered		802.11n RF Analysis Manager RF Performance Manager RF Security Manager
13JNJ-EY2TJ-76CR3-QXLJ5	XN0803091BF32	Array Not Discovered		802.11n RF Analysis Manager RF Performance Manager RF Security Manager

Figure 137. Importing Array Licenses

Click **Finish** to complete the import process. Any license that cannot be deployed now either because the Array has not yet been discovered by XMS or because the array is off line will be placed in the pending list and will be deployed when the Array is available. The **Status** field will show the results for each Array.

Editing Array Licenses

To modify licenses, first display the Array License Management window in your browser by selecting **Tools > Array License Management** from the **Menu Bar** on top of **The XMS Java Client Interface**. (Figure 138) Click the **Licenses** link on the left, and then click the **Edit** link that appears underneath to display all deployed licenses. (Figure 138)



1 Select Arrays 2 Edit Licenses 3 Deploy Licenses

< Previous Next >

Select the arrays for which you wish to edit licenses and click Next.

Select Columns

Showing 1 to 8 of 8 Rows: 25 << < 1 > >>

<input type="checkbox"/>	Status	Hostname	IP Address	Location	Model	Stations	Software Version	Gig1 Mac Address
<input checked="" type="checkbox"/>		Location-Lobby	10.100.46.239	test	XN16	0	5.0.0 (Oct 06 2010), Build: 1531	00:0f:7d:00:d2:a2
<input checked="" type="checkbox"/>		Location-QA	10.100.46.237	test	XN4	0	5.0.0 (Oct 06 2010), Build: 1531	00:0f:7d:01:1e:4c
<input type="checkbox"/>		Location-Support	10.100.46.240	test	XN8	1	5.0.0 (Oct 06 2010), Build: 1531	00:0f:7d:00:76:48

Figure 138. Select Array Licenses to Edit

Select the licenses to be edited by checking the box to the left of each desired row. To select all entries at once, click the checkbox in the header row. To deselect all entries, click the checkbox in the header row again. When the desired entries are selected, click the **Next >** button at the top of the page. The Edit Licenses page appears. (Figure 139)

To modify a license, click the Array's **License Key** field and edit it or type the new license into the field. This is the only field that may be edited. Repeat for as many entries as you need to change.

When you are done editing, click the **Finish** button. The license modifications will be deployed to the selected Arrays, and the status of the operation will be displayed for each Array.

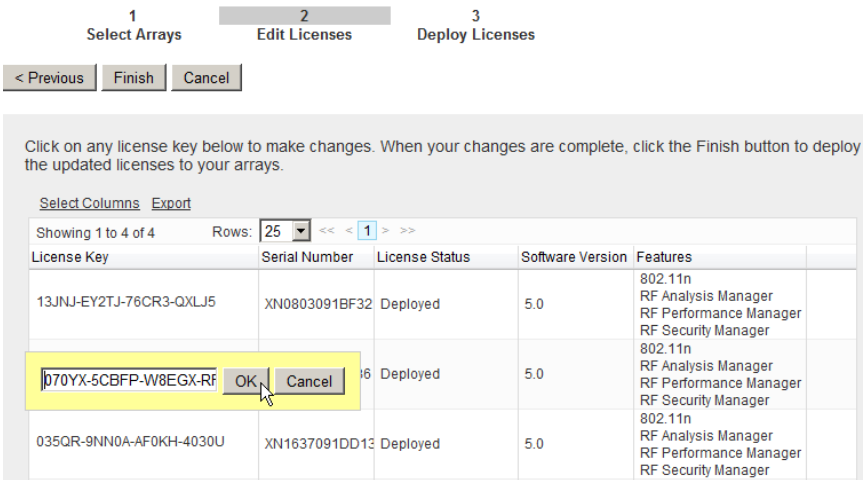


Figure 139. Editing Array Licenses

You may not delete deployed licenses, but you may delete those that have not yet been deployed. See **“Managing Pending Array Licenses” on page 196**.

Also note that you may not enter new licenses “by hand”. To add a new license, please see **“Importing Array Licenses” on page 192**. **“Managing Pending Array Licenses” on page 196**.

Managing Pending Array Licenses

To view licenses that XMS has imported but has not yet been able to deploy, first display the Array License Management window in your browser by selecting **Tools > Array License Management** from the **Menu Bar** on top of **The XMS Java Client Interface**. Click the **Licenses** link on the left, and then click the **Pending** link that appears underneath to display all non-deployed licenses that have been imported. (**Figure 140**)

Note that if an Array is running with a valid license, but a new license was imported for it, it will be listed on both the Deployed Licenses page and the Licenses Pending Deployment page until the new license has been deployed.

Licenses Pending Deployment [\(Click here to view your deployed licenses\)](#)

Deploy Now	Delete	Select Columns	Export		
Showing 1 to 25 of 346				Rows: 25	<< < 1 2 3 4 5 > >>
<input type="checkbox"/>	License Key	Serial Number	License Status	Software Version	Features
<input type="checkbox"/>	1K6QB-2DVX5-RLN05-10001	XN0824081A2E2	Pending Deployment		
<input checked="" type="checkbox"/>	1GHW8-8PH9T-KDH2Q-YMV02	XN0825081A4CB	Array Not Discovered	v5.0	802.11n RF Analysis Manager RF Performance Manager RF Security Manager
<input checked="" type="checkbox"/>	17MU8-80FDX-RQX4G-D2GK0	XN0826081A4E5	Array Not Discovered	v5.0	802.11n RF Analysis Manager RF Performance Manager RF Security Manager
<input type="checkbox"/>	035V5-U1DX8-3D50H-V4RYN	XN0834081A9C5	Array Not Discovered	v5.0	802.11n RF Analysis Manager RF Performance Manager RF Security Manager

Figure 140. Array Licenses Pending Deployment

License Status may have the following values:

- **Array Not Discovered**—a new license that has not been installed because the designated Array has not been discovered yet (i.e., the Array is not listed in the **Discover Devices Window**). This does not mean that XMS cannot find the Array in your network, but rather that the discovery process has not yet added it. To add the Array to XMS, see **“Adding an Array or PoGE Injector” on page 87** or **“Adding a Network” on page 78** or **“Rediscovering a Network” on page 85**. When the Array is discovered, XMS will automatically check whether there is a license pending for it and if so, will attempt to deploy it.

- **Invalid License Key**—the license is not valid. You may edit the License Key as described in [“Editing Array Licenses” on page 194](#). Use the **Deploy Now** button to “push” the corrected license to the Array.
- **Pending Deployment**—a previously discovered Array is currently unreachable or down, and XMS cannot deploy the license.

You may use the **Deploy Now** or **Delete** buttons to manage licenses. Select the desired licenses by checking the box to the left of each desired row. To select all entries at once, click the checkbox in the header row. To deselect all entries, click the checkbox in the header row again.

You may click the **Deploy Now** button at the top of the page to have XMS immediately attempt to deploy the selected licenses on their respective Arrays. You will be informed of the results of the operation. The **License Status** field will show the results quickly, typically well within a few minutes. If successful, the entry will be moved to the list of deployed licenses. The Array is not rebooted but the radios will go down and up, so that station associations will be disrupted briefly. The Array will start using the new license, and will support the capabilities shown in the **Features** column.

You may click the **Delete** button to remove the selected pending licenses. (Deployed licenses may **not** be deleted.)

You may click the **Export** link at the top of the page to export all pending licenses. It is not necessary to select any entries first—all pending licenses will be exported. To export an .xls file, click the **Excel** radio button. To export a file of comma-separated values (.csv), click the **Csv** radio button. Then click **Export**. The File Download dialog box will allow you to open the file, or save it to the location you select.

IAPs

This section discusses the individual IAPs (Integrated Access Points) within each Array that is configured as part of your managed network.

The IAPs Window

This window opens when you click on the **IAPs** node in the **Tree**, which appears under the **Resource** parent node. The IAPs window includes a list of all IAPs included in the Arrays that are part of the Array group selected on the Dashboard. Use the **IAP Status** buttons to filter the IAPs to display only those with a particular status. To search for a particular IAP, see [“Using the Search Feature in the Resource Windows” on page 164](#).

Information on this window is automatically refreshed every 20 seconds.

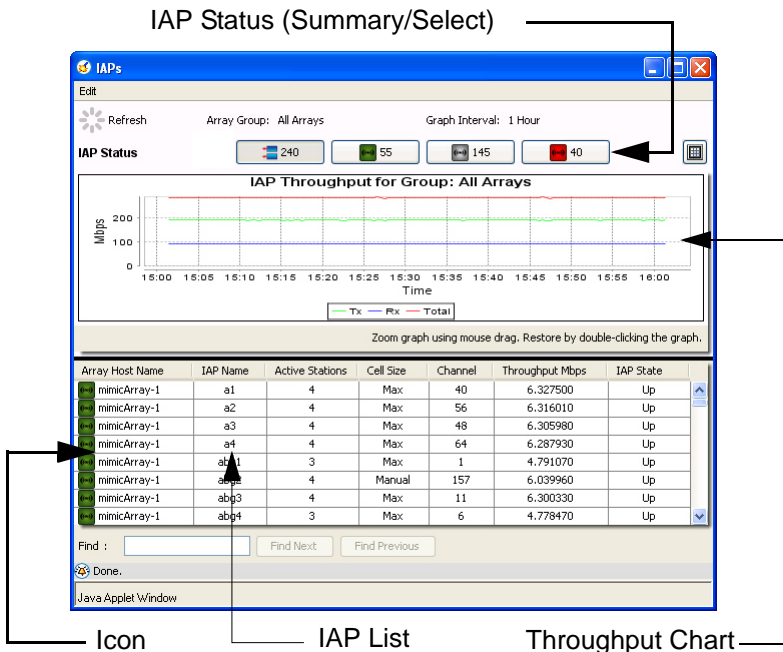


Figure 141. IAPs Window

The IAPs window is divided into three sections:

- **IAP Status**—The buttons show a count of IAPs by status (All IAPs, or Up, Down, or Disabled). Hover the mouse over a button to display the status value represented by the button. Click a button to show only IAPs with the selected status in the IAPs list. This section is similar to Array Status. See [“Array Status” on page 167](#) for details.
- **All IAP Throughput**—a chart of IAP throughput. You may zoom in on a graph region by clicking and dragging the mouse over it; double click anywhere to revert to the full chart. The time interval shown is determined by Performance chart in the Dashboard (see [“Performance” on page 98](#)). This chart is similar to Array Throughput, and data is included only for IAPs shown in the IAP list. See [“Array Throughput” on page 168](#) for details.
- **IAP List**—A list of IAPs, which allows you to perform a number of operations on a selected IAP.

IAP List

The list in the bottom half of the IAPs window contains information about each IAP and the Array to which it belongs. Only IAPs on Arrays that belong to the Array group selected on the Dashboard window are included. You may customize the columns shown in this list—see [“Choosing the Columns for Display” on page 163](#). By default, information is shown about the IAP’s state, the number of active stations associated to the IAP, and its throughput. You may right-click on an IAP to display a menu that allows you to perform the following operations:

- **Web Management**—opens the Array’s Web Management Interface. See [“Connecting to an IAP’s Array” on page 200](#).
- **Configure**—Opens an **IAP Settings** window to allow you to apply configuration changes to the IAP. See [“Configuring the RF Settings of an IAP” on page 200](#).
- **Alarms and Events**—Shows a count of events and alerts for this IAP. See [“Viewing Events and Alerts \(IAPs\)” on page 202](#).

For specific information about IAPs and how they are configured, refer to the *Wi-Fi Array User's Guide*, part number 800-0006-001.

Sorting the List of IAPs

To change how the table is sorted, click in any column header to define that header as the sort criteria. In addition, you can choose to have the results displayed in ascending or descending order, represented by the appropriate arrow icon. To do this, simply click in the same header again to toggle between ascending and descending order.

Connecting to an IAP's Array

To connect to an Array that contains a specific IAP, right-click on the IAP in the IAPs window, then choose **Web Management** from the pull-down list.

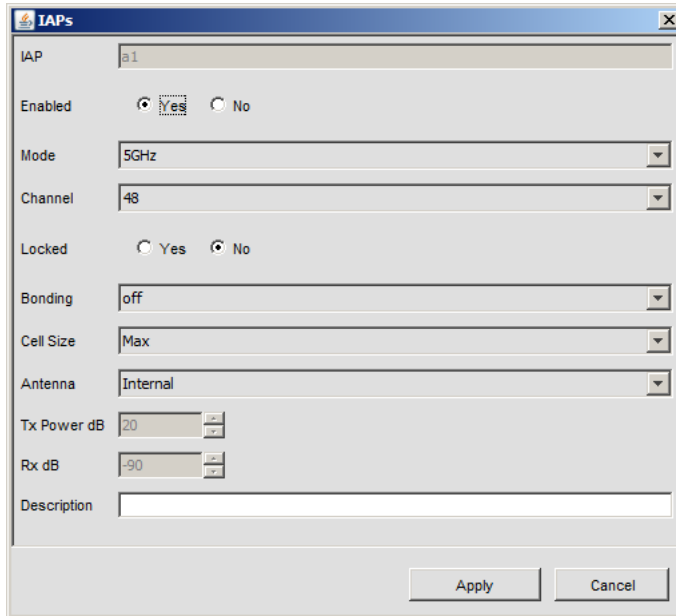
The associated Array's Web Management Interface login window is displayed as a separate window (not part of the XMS client interface). From here you can log in to the Array and proceed as described in [“Connecting to an Array” on page 172](#).

Configuring the RF Settings of an IAP

To open a window to configure the RF settings for a specific IAP ([Figure 142](#)), use any of the following procedures:

- Double-click on the IAP in the IAPs window.
- Right-click on the IAP in the IAPs window, then choose **Configure** from the pull-down list.

When the IAP Settings window is presented, double-click the desired IAP. The configuration options for a selected IAP are identical to the configuration options presented to you when creating IAP and RF configuration policies. To avoid repetition, refer to [“IAPs” on page 309](#) and [“RF” on page 316](#) when configuring the settings for a specific IAP. The two differences between this window and the corresponding policy creation window are the inclusion of an **Execute** button, and the fact that this window shows the currently configured values on the IAP. When you are finished making changes, click on the **Execute** button to apply your new settings.



The screenshot shows a window titled "IAPs" with a list of IAPs. The first IAP is "a1". Below the list, there are several configuration options for the selected IAP:

- Enabled:** Radio buttons for "Yes" (selected) and "No".
- Mode:** A dropdown menu set to "5GHz".
- Channel:** A dropdown menu set to "48".
- Locked:** Radio buttons for "Yes" and "No" (selected).
- Bonding:** A dropdown menu set to "off".
- Cell Size:** A dropdown menu set to "Max".
- Antenna:** A dropdown menu set to "Internal".
- Tx Power dB:** A text input field with "20" and a small up/down arrow.
- Rx dB:** A text input field with "-90" and a small up/down arrow.
- Description:** An empty text input field.

At the bottom right of the window are "Apply" and "Cancel" buttons.

Figure 142. RF Settings

For more information about executing configuration changes, refer to the following:

- [“Executing the Configuration Change” on page 176](#)
- [“Saving Results” on page 176](#)
- [“What if the Configuration Changes are Rejected?” on page 176](#)

Viewing Events and Alerts (IAPs)

To view a summary of events and alerts for the Array to which an IAP belongs, select and then right-click the IAP and choose **Alarms and Events** from the pull-down list. The Events and Alerts summary window for the Array is displayed. For more information about Events and Alerts, see “**Monitoring Your Network**” on page 105.

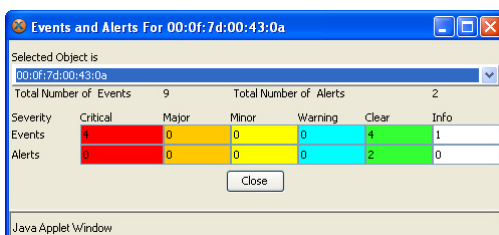


Figure 143. Viewing Events and Alerts

Stations

This section discusses the client stations that are associated to all Arrays within your managed network.

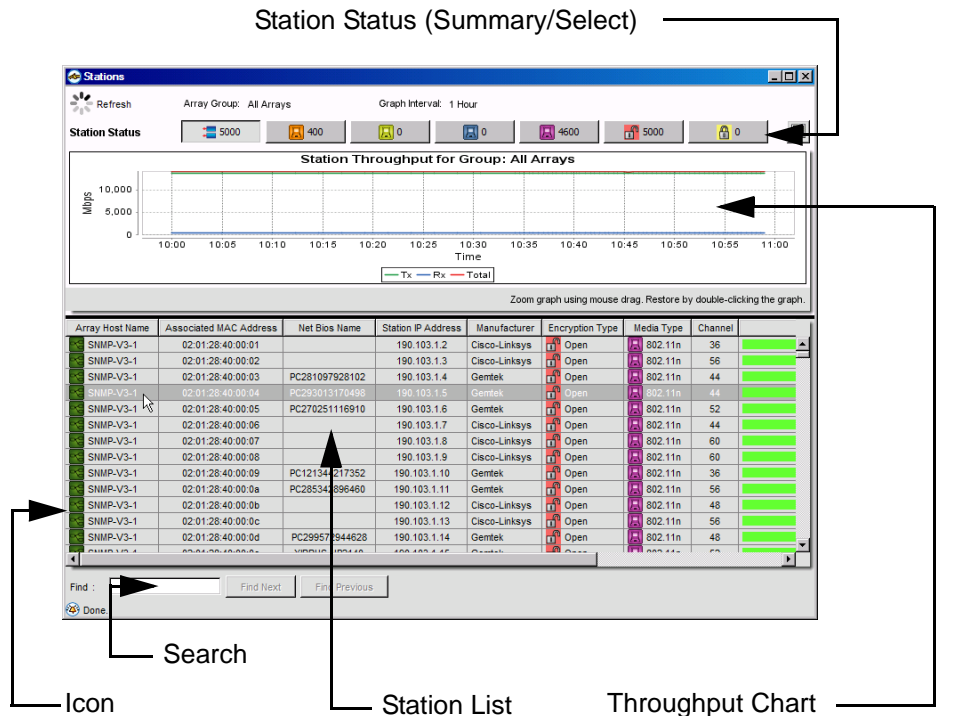


Figure 144. Stations Window

The Stations Window

This window is generated when you click on the **Stations** node in the **Tree**, which appears under the **Resource** parent node. Using the Stations window, you can use the XMS map locationing feature.

The Stations window includes a list of all client stations currently associated to members of the Array group selected on the Dashboard. Information on this window is automatically refreshed every 20 seconds. To search for a particular station in the list, see “Using the Search Feature in the Resource Windows” on page 164.

The Stations window is divided into three sections:

- **Station Status**—The buttons show a count of stations by media (802.11a in orange, 802.11bg in green, 802.11b in blue, or 802.11n in purple), and by encryption type (Open in red, WEP in yellow, and WPA/WPA2 in green). Hover the mouse over a button to display the type of encryption or media represented by the button. Click a button to show only stations of the selected type in the list. Click the leftmost button (Total) to revert to showing all stations.
- **Station Throughput**—a chart of station throughput. You may zoom in on a graph region by clicking and dragging the mouse over it; double click anywhere to revert to the full chart. The time interval shown is determined by the Performance chart in the Dashboard (see [“Performance” on page 98](#)). This chart is similar to Array Throughput, and data is included only for stations shown in the station list. See [“Array Throughput” on page 168](#) for details.
- **Station List**—A list of stations, which allows you to perform a number of operations on a selected station, including finding its location.

Station List

This list shows information about each station and the IAP to which it is associated. Use the **Station Status** buttons to select which stations to display—all stations, or only those with the selected encryption or media type. You may customize the columns shown in this list—see [“Choosing the Columns for Display” on page 163](#). For each station, the following information is shown by default:

- The host name of the Array to which the station is associated.
- The station’s MAC address.
- The **NetBIOS** name of the station.
- The IP address of the station.
- The manufacturer of the station.
- The encryption type (Open, WPA/WPA2, WEP) in use for the connection.
- The media type of the station (802.11n, 802.11a, 802.11b, or 802.11bg).

- The channel being used for the connection.
- The current **RSSI** (signal strength) as measured by the IAP.
- The throughput of the station.
- How long (in days:hours:minutes) the station has been associated to the Array.

You may right-click on a station to display a menu that allows you to perform the following operations:

- **Web Management**—Opens the Array’s Web Management Interface. See [“Connecting to an Associated Array” on page 205](#).
- **Alarms and Events**—Shows a count of events and alerts for this station. See [“Viewing Events and Alerts \(Stations\)” on page 206](#).
- **Locate**—Uses the XMS location algorithm to locate this station on a map. See [“Locating Devices” on page 152](#).

Sorting the List of Stations

To change how the table is sorted, click in any column header to define that header as the sort criteria. In addition, you can choose to have the results displayed in ascending or descending order, represented by the appropriate arrow icon. To do this, simply click in the same header again to toggle between ascending and descending order.

Connecting to an Associated Array

To connect to an Array that a station is associated with, use either of the following procedures:

- Double-click on a station in the Stations window.
- Select and then right-click a station in the Stations window, then choose **Web Management** from the pull-down list.

The associated Array’s Web Management Interface login window is displayed as a new browser window (not part of the XMS client interface). From here you can log in to the Array and proceed as described in [“Connecting to an Array” on page 172](#).

Viewing Events and Alerts (Stations)

To view a summary of events and alerts for the station's associated Array, select and then right-click the station and choose **Alarms and Events** from the pull-down list. The Events and Alerts summary window for the Array is displayed. For more information about Events and Alerts, go to **"Monitoring Your Network"** on page 105.

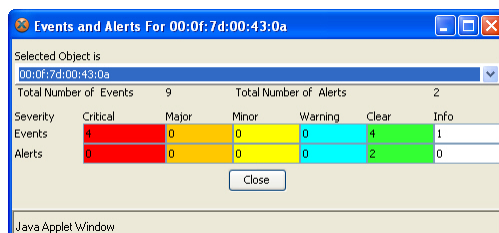


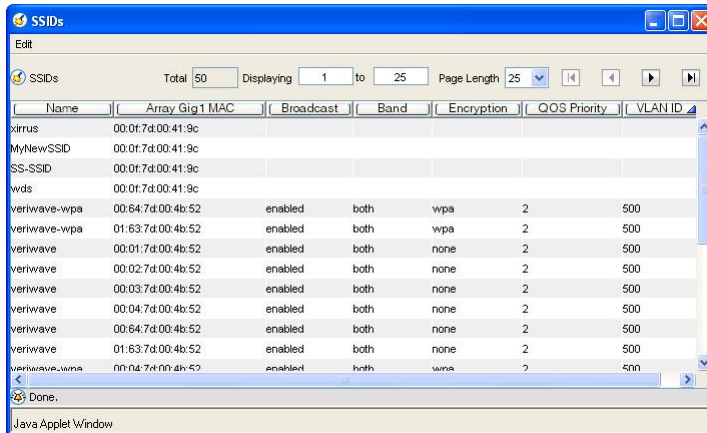
Figure 145. Viewing Events and Alerts

SSIDs

This section discusses the SSIDs that are configured as part of your managed network.

The SSIDs Window

This window is generated when you click on the **SSIDs** node in the **Tree**, which appears under the **Resources** parent node. The SSIDs window includes a list of all SSIDs operating within the network.



The screenshot shows the 'SSIDs' window with a table of SSID configurations. The table has columns for Name, Array, Gig1 MAC, Broadcast, Band, Encryption, QoS Priority, and VLAN ID. The data is as follows:

Name	Array	Gig1 MAC	Broadcast	Band	Encryption	QoS Priority	VLAN ID
xirrus	00:0f:7d:00:41:9c						
MyNewSSID	00:0f:7d:00:41:9c						
SS-SSID	00:0f:7d:00:41:9c						
wds	00:0f:7d:00:41:9c						
veriwave-wpa	00:64:7d:00:4b:52		enabled	both	wpa	2	500
veriwave-wpa	01:63:7d:00:4b:52		enabled	both	wpa	2	500
veriwave	00:01:7d:00:4b:52		enabled	both	none	2	500
veriwave	00:02:7d:00:4b:52		enabled	both	none	2	500
veriwave	00:03:7d:00:4b:52		enabled	both	none	2	500
veriwave	00:04:7d:00:4b:52		enabled	both	none	2	500
veriwave	00:64:7d:00:4b:52		enabled	both	none	2	500
veriwave	01:63:7d:00:4b:52		enabled	both	none	2	500
veriwave-wpa	00:04:7d:00:4b:52		enabled	both	wpa	2	500

Figure 146. SSIDs Window

The SSIDs window contains information about each SSID and the Array it belongs to, as well as informing you whether or not the SSID is being broadcast, the wireless band being used, the encryption type, the QoS priority, and the VLAN ID.

You may right-click on an SSID to display a menu that allows you to perform the following operations:

- **Web Management**—opens the Array’s Web Management Interface. See **“Connecting to an SSID’s Array” on page 208**.
- **Configure**—Opens an **SSID Settings** window to allow you to apply configuration changes to the SSID. See **“Configuring the SSID Settings” on page 208**

- **Alarms and Events**—Shows a count of events and alerts for this SSID. See “**Viewing Events and Alerts (SSIDs)**” on page 210.

For specific information about SSIDs and how they are configured, refer to the *Wi-Fi Array User’s Guide*, part number 800-0006-001.

Sorting the List of SSIDs

To change how the table is sorted, click in any column header to define that header as the sort criteria. In addition, you can choose to have the results displayed in ascending or descending order, represented by the appropriate arrow icon. To do this, simply click in the same header again to toggle between ascending and descending order.

Connecting to an SSID’s Array

To connect to an Array that uses a specific SSID, use either of the following procedures:

- Right-click on an SSID in the SSIDs window, then choose **Web Management** from the pull-down list.

The Array’s Web Management Interface login window is displayed in a new browser window (not part of the XMS client interface). From here you can log in to the Array with your user name and password (the default for both is **admin**), and proceed as described in “**Connecting to an Array**” on page 172.

Configuring the SSID Settings

To configure the settings for a specific SSID, use either of the following procedures:

- Double-click on an SSID in the SSIDs window.
- Right-click on an SSID in the SSIDs window, then choose **Configure** from the pull-down list.

The SSID Settings window is displayed, which contains a list of all SSIDs for an Array. From here you can add, delete or modify an existing SSID.

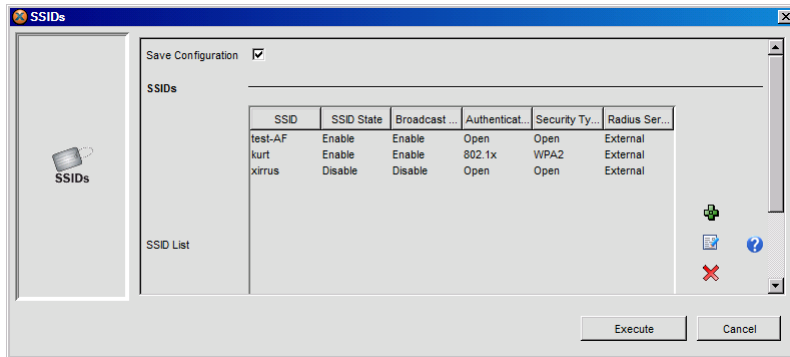


Figure 147. SSID Settings

The configuration options for SSIDs are identical to the configuration options presented to you when creating SSID configuration policies. To avoid repetition, refer to [“SSIDs” on page 287](#) when configuring SSID settings. The two differences between this window and the corresponding policy creation window are the inclusion of an **Execute** button, and the fact that this window shows the currently configured values for this SSID. When finished making changes, click on the **Execute** button to apply your new settings. For more information about executing configuration changes, refer to the following:

- [“Executing the Configuration Change” on page 176](#)
- [“Saving Results” on page 176](#)
- [“What if the Configuration Changes are Rejected?” on page 176](#)

Viewing Events and Alerts (SSIDs)

To view events and alerts for the Array that uses the selected SSID, right-click on the SSID and choose **Alarms and Events** from the pull-down list. The Events and Alerts summary window for the Array is displayed. For more information about Events and Alerts, go to **“Monitoring Your Network” on page 105**.

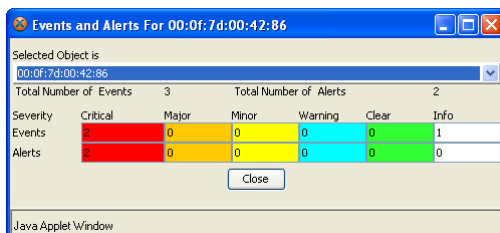


Figure 148. Viewing Events and Alerts

PoGE Injectors

This section provides instructions for managing the Power over Gigabit Ethernet injectors in your Xirrus network. XMS provides a tool for associating PoGE injector ports with the Array ports that they power. Once you have completed this mapping, you may use XMS to monitor the status of injectors and to power down or power-cycle Arrays by controlling the injector ports that drive them.

Managing PoGE injectors with XMS requires the following steps.

1. You **must** set up each injector that will be managed by XMS. The injector must meet these criteria:
 - Must be manageable—must be one of the Xirrus managed PoGE injector models. The injectors use SNMPv2.
 - Must have a static IP address—may be assigned a static address via DHCP or manually.
 - Must be powered on to allow XMS to discover it.
 - All injector configuration may be performed using the injector's Web Management Interface (WMI), as described in the *Power over Gigabit Ethernet Installation and User Guide* (PN 812-0057-001, Rev J or higher).
 - SNMP Community Names must match those expected by XMS for discovery (see **"Adding or Deleting SNMPv2 and SNMPv3 Entries" on page 81**). These strings should be changed from their factory default values to enhance security.
 - (Recommended) The injector's user name and password should be changed from their factory default values to enhance security.

Now you may perform the following steps to start managing the injector with XMS. Each step is described in its own section below.

2. **Add the Injector to XMS**—the XMS Discovery process adds the injector to XMS's managed devices database.
3. **Associate the Injector with an Array**—tell XMS which Array port is connected to each injector output port.

4. **Manage the Injector with XMS**—turn the injector on or off to save power at night or reboot the Array. See “**Managing a PoGE Injector**” on page 187.

Add the Injector to XMS

XMS Discovery can find powered-up Xirrus injectors that are SNMP-capable and are reachable from the networks specified for discovery. The SNMP Community Name of an injector must match one of those listed for SNMPv2. See “**Adding or Deleting SNMPv2 and SNMPv3 Entries**” on page 81.

When the injector has been discovered, it will appear in the Discovered Devices list (**Figure 48 on page 72**), and you may proceed to the next section. If the injector has not yet been discovered, you may enter it manually as described in “**Adding an Array or PoGE Injector**” on page 87.

Associate the Injector with an Array

Once XMS has discovered the injector, you must tell XMS which Array(s) are connected to it. Both the injector and the Array(s) must already be listed in Discovered Devices before you may proceed.


1. From the **Tools** menu, select **PoGE Management**. The PoGE Injector and Array Data and Power Port Mapping window appears.

Step 1: Click on an Injector “Data and Power” port below to begin mapping.


Injector Host Name	IP Address	MAC Address	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7
Xirrus-E00001	10.100.44.30	00:0f:7d:e0:00:01	Mapped to: <input checked="" type="checkbox"/> Oingo Boingo Data and Power Port 1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Xirrus-E00002	10.100.23.42	00:0f:7d:e0:00:02	Mapped to: <input checked="" type="checkbox"/> MB-150-280-AX1 Data and Power Port 1	<input checked="" type="checkbox"/>					
Xirrus-E00007	10.100.40.90	00:0f:7d:e0:00:07	<input checked="" type="checkbox"/>						

Name: MB-150-280-AX1
 Port Number: 1
 IP Address: 10.100.23.51
 MAC Address: 00:0f:7d:00:12:16

Figure 149. Injector and Array Associations

2. Click the **PoGE** link and find the row for the desired injector. The row shows the number of ports on the injector. Note that the icons  indicate ports that are available for connection—injector ports that are not yet

associated with an Array port. If a port already has an association, then the connected Array port is displayed. You may hover the mouse over the port to display the IP and MAC address of the Array being powered by the injector.

Click the icon  for the port that you wish to associate with an Array. The mapping dialog appears.

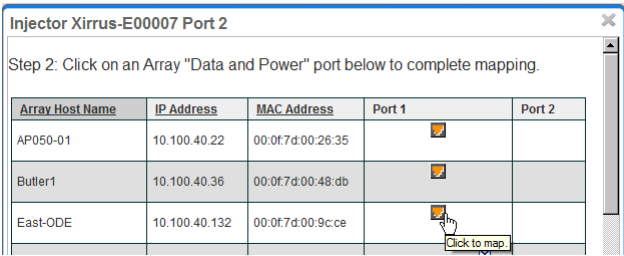





Figure 150. Associating Injector and Array Ports

The mapping dialog lists Arrays, and shows an icon  for ports that have not yet been associated with an injector port. Some older Array models are not directly compatible with Xirrus managed PoGE injector models. Since power for these Arrays cannot be managed with XMS, no port icons are shown for them.

- 3. Find the row for the desired Array. Click the “unused port” icon  for the Array port that is connected to the selected injector port. The PoGE Injector and Array Port Mapping window ([Figure 149](#)) shows the new connection.
- 4. To delete a connection from XMS, click the blue  for that port. To view the associations by Array, click the **Arrays** link on the left.

Manage the Injector with XMS

Once a Xirrus PoGE injector output port has been mapped to an Array port, you may turn the PoGE port on and off, and view its status. This is done via the Array right-click menu on [The Arrays Window](#). See “[Managing a PoGE Injector](#)” on [page 187](#).

Managing Configuration with Policies

This chapter shows you how to use the Java client to create and manage policies for individual Arrays, set up groups of Arrays for convenient management, and how to audit configuration changes. Policies are used by XMS to establish a uniform and efficient method for applying predefined criteria to your Wi-Fi Arrays. For example, if you establish a security policy then all of the parameters you defined for that policy can be easily assigned to any Array or group of Arrays from a menu of security policies. Section headings for this chapter follow the structure of the Configuration node in the Java client's [Tree](#).

- **Working with Policies**
- Policies:
 - “Global Policy” on page 223
 - “System Information” on page 225
 - “Management Control” on page 228
 - “Network” on page 239
 - “Services” on page 247
 - “VLAN” on page 259
 - “DHCP Server” on page 265
 - “Security” on page 270
 - “SSIDs” on page 287
 - “User Groups” on page 301
 - “IAPs” on page 309
 - “RF” on page 316
 - “WDS” on page 342
 - “Filters” on page 348
 - “Software Update” on page 354
 - “Web Page Redirect (WPR)” on page 358

- “Configuration File (Advanced)” on page 362
- “Groups” on page 366
- “Audit” on page 370

Working with Policies

*NOTE: A policy defines the **entire** configuration of an Array feature. When a policy is applied to an Array, any existing configuration is **replaced** with the configuration defined in the policy. For example, an SSID policy defines a set of SSIDs. When an SSID policy is applied to an Array, the Array is set to have **exactly** this set of SSIDs. Thus, any previous SSID configurations on the Array will be deleted, and will be replaced by the set of SSIDs configured in the policy. The only exception to this is the **Configuration File (Advanced)** policy, which makes incremental changes to the settings on an Array when the policy is executed.*

*If you wish to make a change to existing configuration on an Array, rather than replacing that aspect of its configuration, don't use a policy (except for the **Configuration File (Advanced)** policy). Instead, see “**Configuring an Array**” on page 174.*

All policy types reside in the **Tree** under the Configuration node. To expand the node, either double-click on **Configuration** and then on **Policies** or click on the + symbol before these tree nodes.

From the expanded tree, click on any policy type to generate a window that lists all policies for the type of policy you selected. Policies are listed in table form, displaying columns for a default group of the policy's settings, otherwise the general structure of all policy windows is the same. To change the columns displayed for a policy window, go to “**Selecting the Columns Shown in a Policy Window**” on page 220.

An Easy Way to Work With Policies

XMS has a feature that allows you to “pull” or read the existing configuration of any Array, and create policies that mirror that configuration. These policies may then be applied to other Arrays in the **Managed Network** to easily configure them and ensure a uniform configuration across the Wi-Fi network.

You may even select the option to automatically create a **Global Policy** that groups together all of the individual policies pulled from the example Array. Then you may apply the global policy to an Array to configure it to match the example Array in one step.

There are two ways to create a policy based on the configuration of an Array:

- From a policy window, click **Add Policy**. An Add Policy dialog box appears, allowing you to create a new policy based on one of the listed Arrays. See **“Adding a Policy” on page 219**.
- From the **Arrays** window, you may select which policies to read from the Array, and you may edit them later following the instructions for each policy type in this chapter. See **“Create Policies from Array” on page 178** for details.

Using Policy Windows

Policy windows are active windows, providing buttons that allow you to add a new policy, modify or delete an existing policy, or change the columns displayed on the policy window. In addition, most policy windows provide a convenient method for executing a chosen policy on multiple Arrays within the network.

To avoid repetition, **Figure 151** shows an example of a standard policy window highlighting the active areas of the window. In this example, the Security Policy window is used.

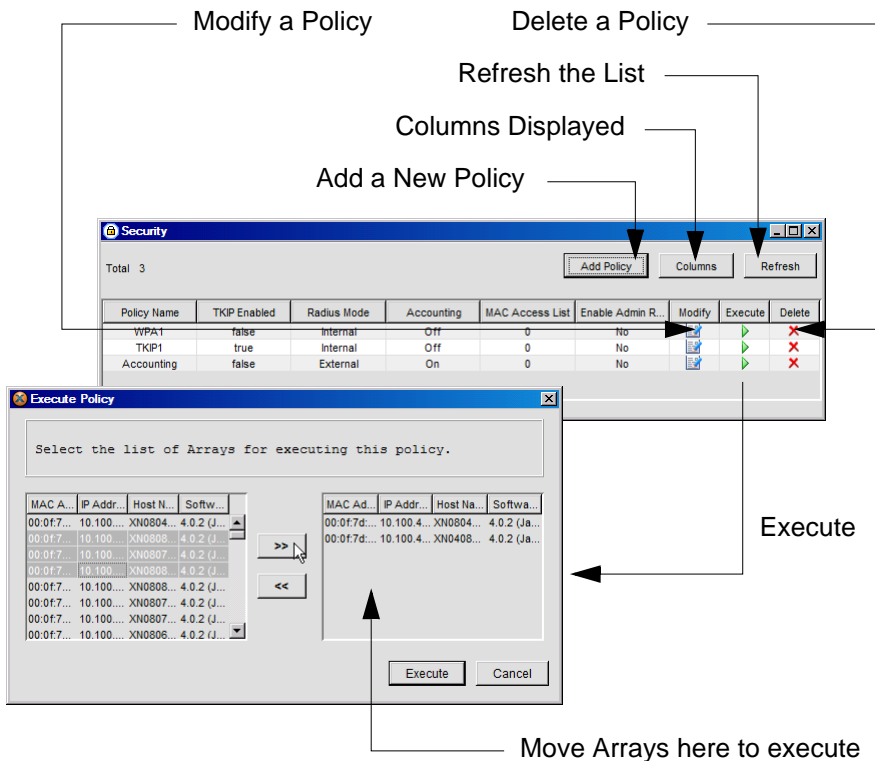


Figure 151. Policy Window - Executing a Policy

Adding a Policy

To create a new policy in any policy window, click the **Add Policy** button. Most of the Add Policy windows will offer you a choice between creating the policy from scratch or by copying the configuration from a “model” Array. Copying the policy from the configuration of an Array is strongly recommended in most cases. It allows you to try out the configuration in your network and prove that it operates as intended, before executing the policy against a number of Arrays. It also allows you to make sure that you have configured all policy settings correctly, without omitting any or causing conflicts with other settings.

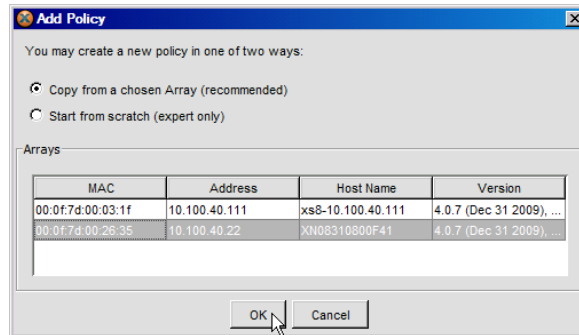


Figure 152. Adding a Policy

- **Copy from a chosen Array (recommended)**

Choose this option to create the new policy by copying its settings from an Array. Select an Array from the list and click **OK**. The Policy Details window will appear, with the new policy having the same name as the model Array. You may edit any of the fields that appear in this window as needed, including the **Policy Name**.

You may create any type of policy by copying from an Array, except for the **Global Policy**, **Software Update**, and **Web Page Redirect (WPR)** policies. For these policies, you are not offered the choice of copying the policy from an Array. The Policy Details window will appear by default, without having to click through from the Add Policy window first.

- **Start from scratch (expert only)**

If you choose this option, the Policy Details window will appear. It will show exactly the same fields as it would if you chose to create the new policy by copying, but they will all be blank. Only expert users should choose this option, since it is easier to enter settings that are not appropriate for your network this way.

Selecting the Columns Shown in a Policy Window

Click the **Columns** button to change the information displayed for the policy list. The Select Policy Attributes window will appear.

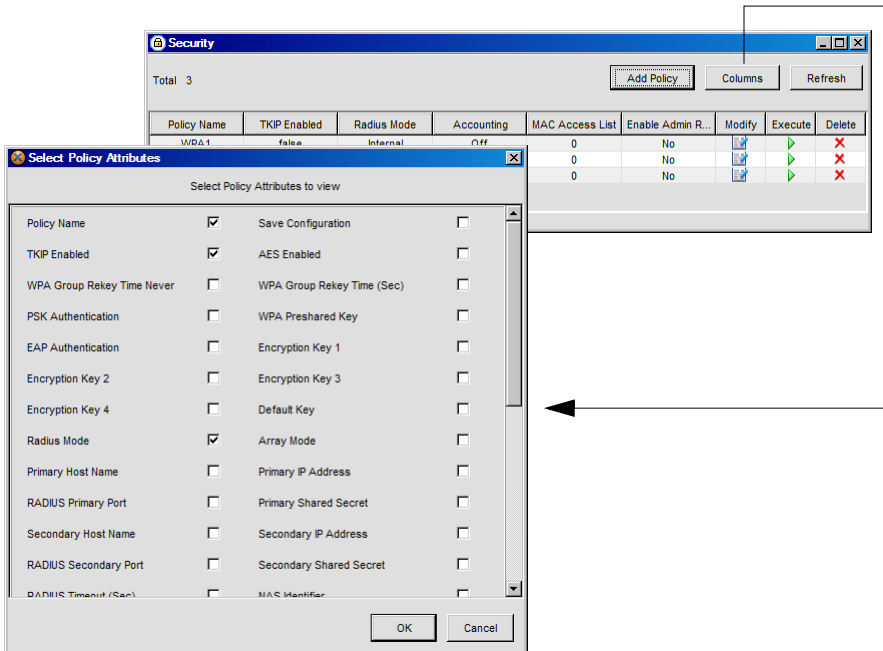


Figure 153. Selecting the Attributes of a Policy Window

This window allows you to check (or uncheck) boxes to define the columns that are displayed in the policy window. For example, under Security Policy, if you check the **AES Enabled** box, then a column is displayed showing the setting for each policy for the AES Enabled field (either True or False). If you uncheck the

box, the column is removed from the policy window. This feature provides a convenient at-a-glance method for viewing the settings of each policy listed in the Policy window.

To generate the Select Policy Attributes window for any policy window, open that window and then click on the **Columns** button.

Refreshing the List

The information contained in any policy window can be refreshed by clicking on the **Refresh** button (refer to [Figure 151](#) to locate the button). When you refresh the list, all information in the window is updated to the current active state.

Modifying an Existing Policy

This chapter documents the creation of new policies for all policy types. It does not document how to modify an existing policy for each type, because the procedure is the same for all policies. Use either of the following two methods to access the configuration window used by the policy:

- Double-click on the policy in the policy window.
- Click on the policy to select it, then click on the **Modify** button.

You can now make changes to the properties of the policy. It makes no difference whether the policy was created by copying it from an Array, or entered from scratch—both may be edited. If you need guidance for making your changes, refer to the section in this chapter that documents the creation of a new policy for the policy type you want to modify. Policy names cannot be changed on existing policies.

Executing a Policy

To apply a policy to one or more Arrays, click the green arrow in the Execute column for the desired policy. ([Figure 151](#)) The Execute Policy window appears. Select the desired Arrays from the list on the left, and click >> to move them to the list on the right. You may sort the entries using the column header of any column. You may select multiple entries using **Ctrl+Click**, **Shift+Click**, or **Ctrl+a**. Click the **Execute** button to apply the policy to the Arrays listed on the right.

For increased efficiency, the policy is applied to a number of Arrays simultaneously—up to 40 at once. This allows large networks to be upgraded up to forty times faster, compared with applying the policy to one Array at a time. Thus if you have selected 80 Arrays, the policy will be pushed out to them in two rounds of 40 each.

Deleting an Existing Policy

The procedure for deleting a policy is the same for all policies. Simply click on the policy to select it, then click on the **Delete** button. At the confirmation dialog, click on the **Yes** button to confirm the delete action.

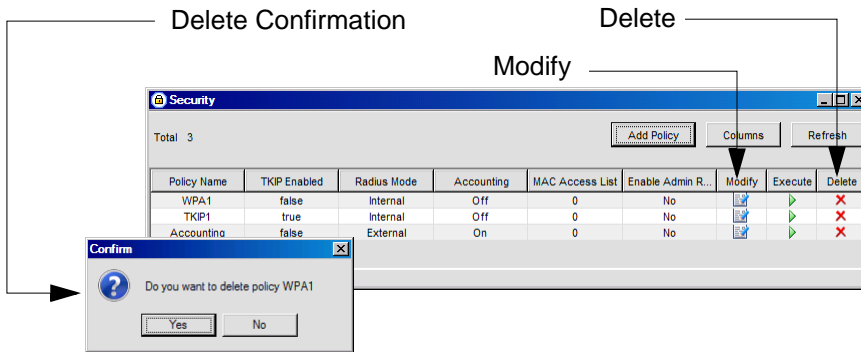


Figure 154. Modifying and Deleting a Policy

Global Policy

A **Global Policy** allows you to select a set of policies that can be applied to Arrays in one shot. It is simply a convenience that applies a set of policies in one step, rather than one at a time. It simplifies Array management by defining a set of policies that set a desired Array configuration. Different global policies may be created for different configurations that you commonly use. Global Policies were previously called default policies.

From the **Configuration>Policies** node in the tree, click on **Global Policy** to display the Global Policy window. This window contains a list of all global policies currently available to be applied to Arrays or groups, with tools to manage these policies.

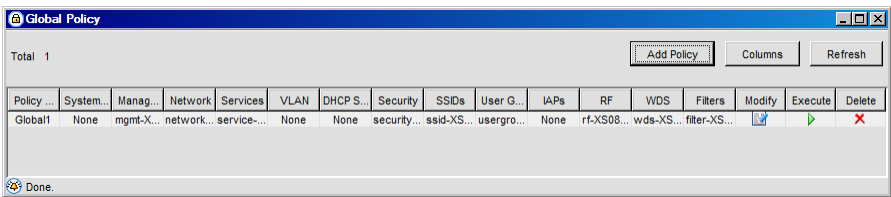


Figure 155. List of Global Policies

The columns in this window show selected settings for the listed policies. For information about changing the columns displayed, see [“Selecting the Columns Shown in a Policy Window” on page 220](#).

Creating a New Global (Default) Policy

To create a new global (default) policy, click on the **Add Policy** button in the Global Policy window.

Global Policy Settings

This window contains a field for defining the name of the policy, and fields for choosing policies from the pull-down lists in each policy category.

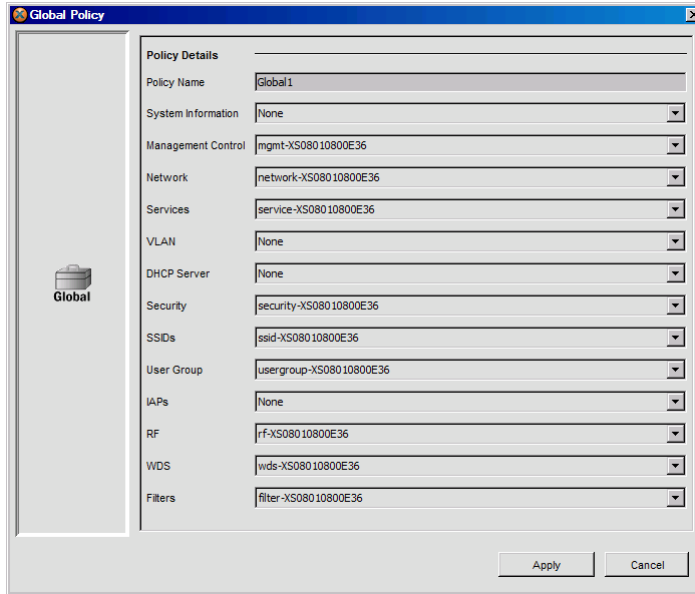


Figure 156. Global (Default) Policy Settings

Policy Details

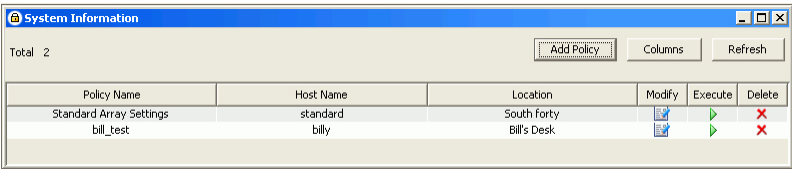
- Policy Name**
Enter a meaningful name that describes this global policy. If you are modifying an existing policy this field is grayed out (not editable). If you are using a standard naming convention for all of your policies, the name you enter here should conform to that convention.
- All Policy Types**
Choose a policy from the pull-down list for any policy type available in this window.

Saving Your Global Policy

When finished, click on the **Apply** button in the Global Policy Settings window to save the new policy.

System Information

From the **Configuration>Policies** node in the tree, click on **System Information** to display the System Information window. This window contains a list of all server policies currently available, with tools to manage these policies.



The screenshot shows a window titled "System Information". At the top left, it says "Total: 2". To the right are buttons for "Add Policy", "Columns", and "Refresh". Below these is a table with the following data:

Policy Name	Host Name	Location	Modify	Execute	Delete
Standard Array Settings	standard	South Forty			
bill_test	billy	Bill's Desk			

Figure 157. List of System Policies

The columns in this window show selected settings for the listed policies. For information about changing the columns displayed, see [“Selecting the Columns Shown in a Policy Window” on page 220](#).

Creating a New System Policy

A system policy is created so that you can configure system and management options. To create a new system policy, click the **Add Policy** button in the System Policy window. When the Add Policy window appears, select **Copy from a chosen Array (recommended)** and choose a model Array, or select **Start from scratch**, as described in [“Adding a Policy” on page 219](#). Click OK.

The System Information window is displayed, with two areas:

- **Policy Details**
Allows you to associate settings with a named policy.
- **System Settings**
Allows you to establish the basic system and administration information.

This window contains a field for defining the name of the policy and fields for configuring the host name, location and contact information.

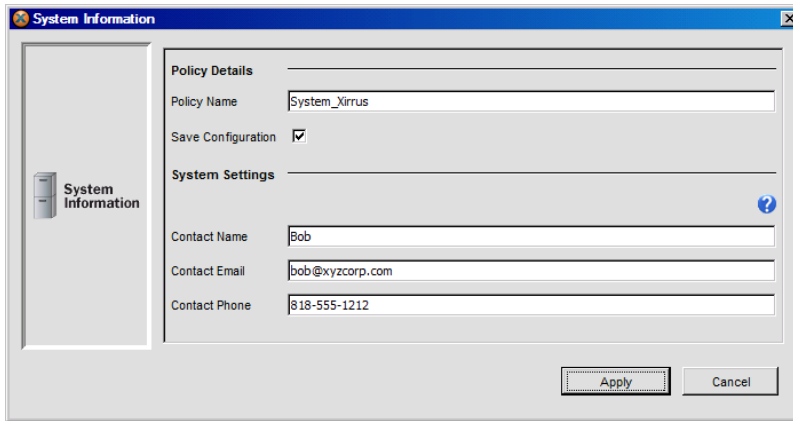


Figure 158. System Settings

Policy Details

- **Policy Name**

Enter a meaningful name that describes this policy. If you are modifying an existing policy this field is grayed out (not editable). If you are using a standard naming convention for all of your policies, the name you enter here should conform to that convention.

- **Save Configuration**

Check this box to ensure that any time this policy is applied to an Array, the Array will save the updated configuration information to its flash memory. If this box is left unchecked, then when this policy is applied to Arrays the configuration changes will need to be saved manually or else they will be lost when the Arrays are rebooted. Note that this checkbox does not actually apply the policy to any Arrays. To apply the policy, see [“Using Policy Windows” on page 218](#).

System Settings

- **Contact Name**
Enter the name and contact information of the person who is responsible for administering the Array at the designated location.
- **Contact Email**
Enter the email address of the administrator.
- **Contact Phone**
Enter the telephone number of the administrator.

Saving Your System Information Policy

When you have configured all of your system information settings, click on the **Apply** button in the System Information window to save the new policy.

Management Control

From the **Configuration>Policies** node in the tree, click on **Management Control** to display the Management Control window. This window contains a list of all management policies currently available, with tools to manage these policies.

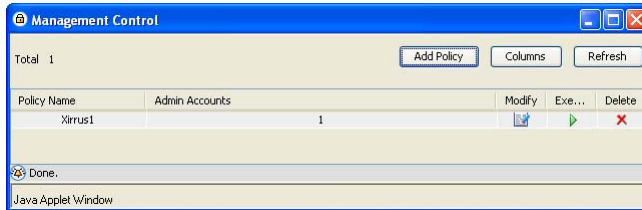


Figure 159. List of Management Policies

The columns in this window show selected settings for the listed policies. For information about changing the columns displayed, see [“Selecting the Columns Shown in a Policy Window” on page 220](#).

Creating a New Management Policy

A management policy is created so that you can set up management access and control. To create a new management policy, click on the **Add Policy** button in the Management Control list window. When the Add Policy window appears, select **Copy from a chosen Array (recommended)** and choose a model Array, or select **Start from scratch**, as described in [“Adding a Policy” on page 219](#). Click **OK**.

The Management Control window is displayed, which is divided into four primary areas:

- **Management Settings**
Allows you to define and configure different management options, including Telnet, SSH and HTTPS.
- **SNMP**
SNMP (Simple Network Management Protocol) server allows remote management of the Arrays by XMS or other SNMP-based management systems. This window configures SNMPv2 and SNMPv3, including setting the Trap Hosts used by both SNMP versions.

- **Admin**

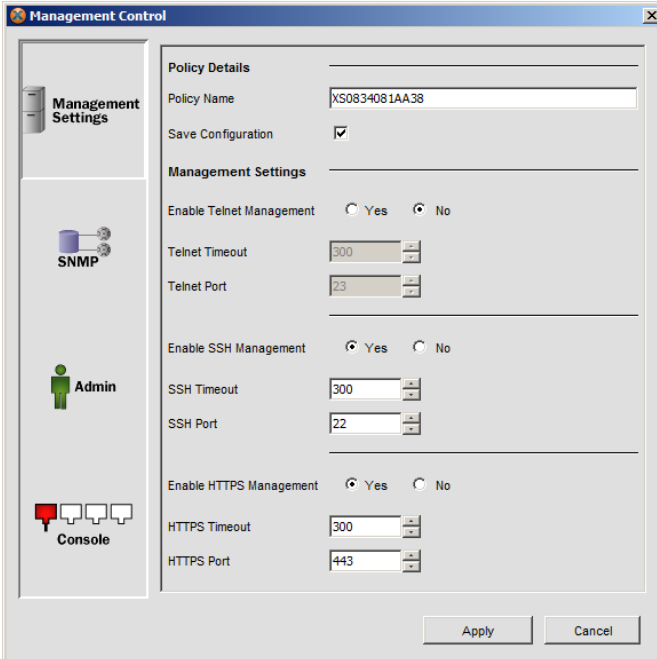
Allows you to create and maintain administrator accounts.

- **Console**

The console (serial) interface is used for connecting directly with an Array's Command Line Interface (CLI) via HyperTerminal. This is useful when an Array's IP address is unknown or a network connection has been lost.

Management Settings

This window contains fields for configuring the Telnet, SSH and HTTPS management options.



The screenshot shows the 'Management Control' window with the 'Management Settings' tab selected. The left sidebar contains icons for 'Management Settings', 'SNMP', 'Admin', and 'Console'. The main area is divided into 'Policy Details' and 'Management Settings' sections.

Policy Details	
Policy Name	XS0834081AA38
Save Configuration	<input checked="" type="checkbox"/>

Management Settings	
Enable Telnet Management	<input type="radio"/> Yes <input checked="" type="radio"/> No
Telnet Timeout	300
Telnet Port	23
Enable SSH Management	<input checked="" type="radio"/> Yes <input type="radio"/> No
SSH Timeout	300
SSH Port	22
Enable HTTPS Management	<input checked="" type="radio"/> Yes <input type="radio"/> No
HTTPS Timeout	300
HTTPS Port	443

At the bottom right are 'Apply' and 'Cancel' buttons.

Figure 160. Management Settings

Policy Details

- **Policy Name**

Enter a meaningful name that describes this policy. If you are modifying an existing policy this field is grayed out (not editable). If you are using a standard naming convention for all of your policies, the name you enter here should conform to that convention.

- **Save Configuration**

Check this box to ensure that any time this policy is applied to an Array, the Array will save the updated configuration information to its flash memory. If this box is left unchecked, then when this policy is applied to Arrays the configuration changes will need to be saved manually or else they will be lost when the Arrays are rebooted. Note that this checkbox does not actually apply the policy to any Arrays. To apply the policy, see ***“Using Policy Windows” on page 218.***

Management Setting Details



*If you choose to modify any of the port assignments below, please ensure that they do not interfere with any of the required ports used by XMS and by Arrays. Please see **“XMS Port Requirements” on page 22** for details.*

- **Enable Telnet Management**

Choose **Yes** to enable management using Telnet, or choose **No** to disable Telnet management. The default is No.

Be aware that Telnet is not secure over network connections and should be used only with a direct port connection. When connecting to the Command Line Interface over a network connection, you must use a Secure Shell (SSH) utility. The most commonly used freeware providing SSH tools is PuTTY.

- **Telnet Timeout**

Enter the maximum idle time (in seconds) before the Telnet session times out. The default is 300 seconds.

- **Telnet Port**
If you wish to change the port used for Telnet from the default value (23), enter the desired port number here.
- **Enable SSH Management**
Choose **Yes** to enable management using a Secure Shell (SSH) utility, or choose **No** to disable SSH management. The default is Yes.
- **SSH Timeout**
Enter the maximum idle time (in seconds) before the SSH session times out. The default is 300 seconds.
- **SSH Port**
If you wish to change the port used for SSH from the default value (22), enter the desired port number here.
- **Enable HTTPS Management**
Choose **Yes** to enable management using a secure Web browser via HTTPS (HyperText Transmission Protocol, Secure), or choose **No** to disable HTTPS management. The default is Yes.

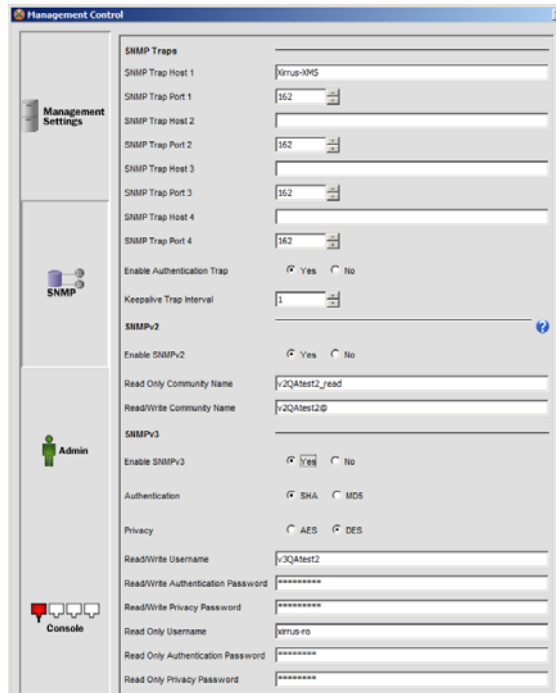
Arrays may be managed using Internet Explorer (version 7.0 or higher), Mozilla Firefox (version 3.0 or higher), Chrome (version 3.0 or higher), or Safari (version 5.0 or higher). A secure Web browser is required for Web-based management of Arrays.
- **HTTPS Timeout**
Enter the maximum idle time (in seconds) before the HTTPS session times out. The default is 300 seconds.
- **HTTPS Port**
If you wish to change the port used for HTTPS from the default value (443), enter the desired port number here.

SNMP

NOTE: To manage your Arrays with XMS, it is very important to use the correct **SNMPv2 Read-Write Community String** or **SNMPv3 Settings authentication** information for proper operation of XMS with the Array. Both XMS and the Array must have the same settings for the SNMP version being used.

About SNMP v2 and SNMP v3

XMS supports both Version 2 and Version 3 of SNMP. SNMPv3 is preferred for the higher level of security it provides. When XMS is discovering Xirrus Arrays and PoGE injectors, it attempts contact via SNMPv3 first. SNMPv2 is tried next. Discovery records which SNMP version was used to find a Xirrus device, and XMS uses that version for management thereafter. Arrays support both SNMPv2 and v3; injectors support SNMPv2 only. See “[Adding or Deleting SNMPv2 and SNMPv3 Entries](#)” on page 81.



SNMP Traps	
SNMP Trap Host 1	xirrus-xms
SNMP Trap Port 1	162
SNMP Trap Host 2	
SNMP Trap Port 2	162
SNMP Trap Host 3	
SNMP Trap Port 3	162
SNMP Trap Host 4	
SNMP Trap Port 4	162
Enable Authentication Trap	<input checked="" type="radio"/> Yes <input type="radio"/> No
Keepalive Trap Interval	1
SNMPv2	
Enable SNMPv2	<input checked="" type="radio"/> Yes <input type="radio"/> No
Read Only Community Name	jv2QAtest2_read
Read/Write Community Name	jv2QAtest2@
SNMPv3	
Enable SNMPv3	<input checked="" type="radio"/> Yes <input type="radio"/> No
Authentication	<input checked="" type="radio"/> SHA <input type="radio"/> MD5
Privacy	<input type="radio"/> AES <input checked="" type="radio"/> DES
Read/Write Username	jv2QAtest2
Read/Write Authentication Password	*****
Read/Write Privacy Password	*****
Read Only Username	xirrus-ro
Read Only Authentication Password	*****
Read Only Privacy Password	*****

Figure 161. SNMP Settings

SNMP Settings

This window ([Figure 161](#)) has three sections:

- **SNMP Trap Settings**—configures traps sent by Arrays for both SNMPv2 and SNMPv3.
- **SNMPv2 Settings**—enables SNMPv2 and sets the SNMPv2 Community Names on Arrays.
- **SNMPv3 Settings**—enables SNMPv3 and sets the SNMPv3 authentication parameters on Arrays.

SNMP Trap Settings

- **SNMP Trap Hosts (1 to 4)**
Enter the IP address of an SNMP management station that is to receive SNMP traps. You may specify up to four hosts that are to receive traps. If you want XMS to receive traps from the device, enter the XMS server's IP address. (SNMP v2 and v3)
- **SNMP Trap Ports (1 to 4)**
Enter a value in this field to define the SNMP trap port for each of the trap hosts that you entered, or increment/decrement the value using the UP and DOWN arrows. The default is 162. (SNMP v2 and v3)
- **Enable Authentication Trap**
Choose **Yes** to log authentication failure traps, or choose **No** to disable this feature. Enable this feature to configure any of the Trap Hosts below. (SNMP v2 and v3)
- **Keepalive Trap Interval (in minutes)**
The Array sends keepalive traps (sometimes called the phone home trap) to the XMS server. This prompts the server to automatically discover the Array if it has not already been discovered. The interval between traps defaults to once a minute, but once XMS discovers the device it reduces down to once an hour. Keepalive traps are not stopped altogether in the event that the XMS database is lost—all devices will automatically be repopulated by the keepalive traps in this case.
The default value is 1. (SNMP v2 and v3)

SNMPv2 Settings

- **Enable SNMP**
This enables SNMPv2. Either SNMPv2 or SNMPv3 or both **must** be enabled on Arrays to allow management via XMS.
- **SNMP Read-Only Community String**
Enter the read-only community string. The default is **xirrus_read_only**. (SNMP v2)
- **SNMP Read-Write Community String**
Enter the read-write community string. The default is **xirrus**. (SNMP v2)

SNMPv3 Settings

The SNMPv3 section configures authentication and other security settings required to allow XMS to manage the Array using the stronger security provided by SNMPv3.

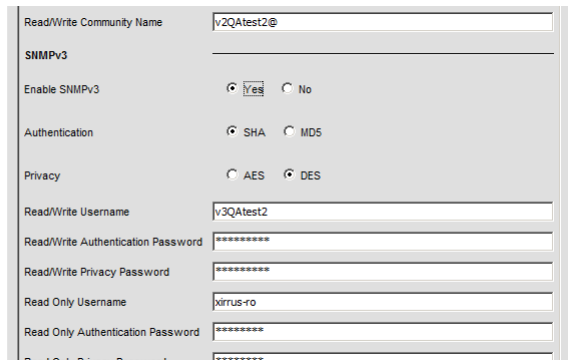


Figure 162. SNMPv3 Settings

- **Enable SNMPv3**
Choose **Yes** to enable SNMP v3 functionality, or choose **No** to disable this feature. Either SNMPv2 or SNMPv3 or both **must** be enabled on Arrays to allow management via XMS. The default for this feature is **No** (disabled).
- **Authentication**
Select the desired method for authenticating SNMPv3 packets: **SHA** (Secure Hash Algorithm) or **MD5** (Message Digest Algorithm 5).

- **Privacy**
Select the desired method for encrypting data: **DES** (Data Encryption Standard, the default) or the stronger **AES** (Advanced Encryption Standard).
- **SNMP Read-Write Username**
Enter the read-write user name. This username and password allow configuration changes to be made on the Array. The default is **xirrus-rw**.
- **SNMP Read-Write Authentication Password**
Enter the read-write password for authentication (i.e., logging in). The default is **xirrus-rw**.
- **SNMP Read-Write Privacy Password**
Enter the read-write password for privacy (i.e., a key for encryption). The default is **xirrus-rw**.
- **SNMP Read-Only Username**
Enter the read-only user name. This username and password do not allow configuration changes to be made on the Array. The default is **xirrus-ro**.
- **SNMP Read-Only Authentication Password**
Enter the read-only password for authentication (i.e., logging in). The default is **xirrus-ro**.
- **SNMP Read-Only Privacy Password**
Enter the read-only password for privacy (i.e., a key for encryption). The default is **xirrus-ro**.

Admin

This window contains an editable table listing all administrator accounts currently assigned to this policy.

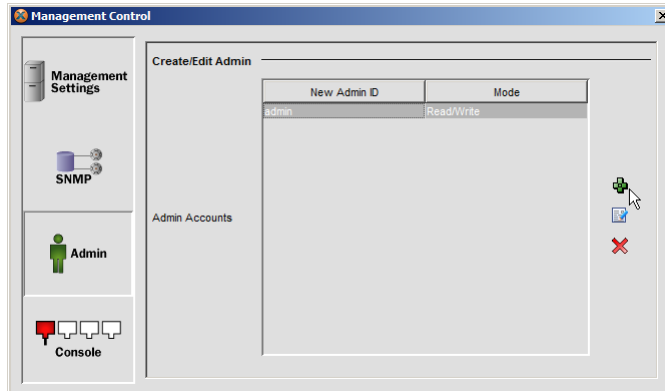



Figure 163. Admin Settings

Create/Edit Admin

To add a new administrator account to the list, click the  button to display the Admin Accounts window.

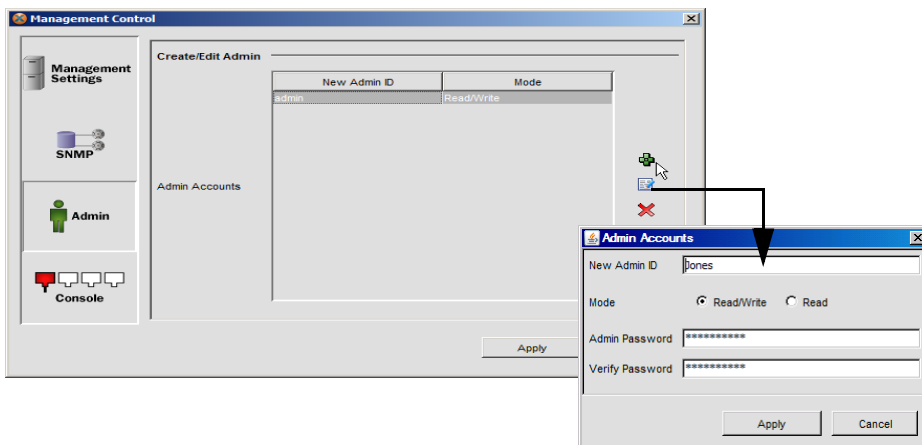


Figure 164. Adding an Administrator Account to the Admin List

- **New Admin ID**
Enter a description for the new administrator account.
- **Mode**
Choose **Read/Write** to grant both read and write privileges to this administrator, or choose **Read** to allow read only privileges (write privileges are denied). The default is Read/Write. In the read only mode, administrators cannot make changes to configurations.
- **Admin Password**
Enter a password for this administrator account ID.
- **Verify Password**
Re-enter the password in this field to verify that you typed the password correctly.

After configuring your administrator accounts, click on the **Add** button. You are returned to the Admin Settings window where the new administrator account is displayed in the list.

Console

This window contains fields for configuring the serial (console) interface's operating parameters.

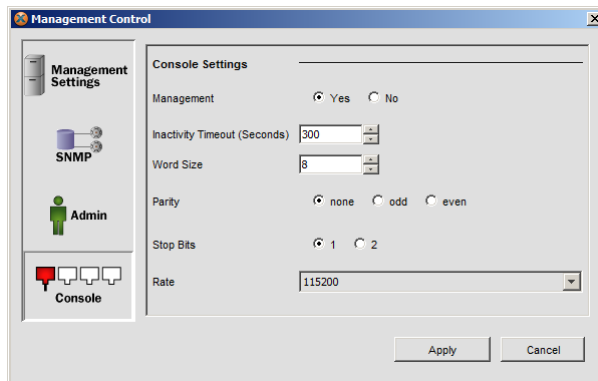


Figure 165. Console Settings

Console Settings

- **Management**

Choose **Yes** to allow management of the Arrays via the serial interface using a HyperTerminal connection to the Command Line Interface, or choose **No** to deny all management privileges for this interface.

- **Inactivity Timeout**

Enter a value in this field to define the elapsed idle time (in seconds) before the connection is dropped, or increment/decrement the time using the UP and DOWN arrows. The default is 300 seconds.

- **Word Size**

Enter a value in this field to define the word size (in data bits), or increment/decrement the value using the UP and DOWN arrows. The default is 8 bits. With the word size set at 8 bits, all communications with the Arrays will use only 8 bit words.

- **Parity**

A parity bit is used to reveal errors in the transfer of data. Even parity means that the parity bit is set so that there are an even number of 1s in the word (see word size). Odd parity means that the parity bit is set so that there are an odd number of 1s in the word. Choose the preferred parity, either **None**, **Odd** or **Even**. The default is None, where no parity checking is performed.

- **Stop Bits**

In asynchronous communications, where every byte of data is preceded by a start bit and followed by a stop bit, the stop bit indicates that a byte has been successfully transmitted. Like parity, stop bits are used for error detection. Choose either **Yes** or **No** for stop bits. The default is No.

- **Rate**

This is the data transmission rate in bits per second (bps). Choose the desired data rate from the pull-down list. The default is 115,200 bps.

Saving Your Management Control Policy

When you have configured all of your management control settings, click on the **Apply** button in the Management Control window to save the new policy.

Network

From the **Configuration>Policies** node in the tree, click on **Network** to display the Network window. This window contains a list of all network policies currently available, with tools to manage these policies.

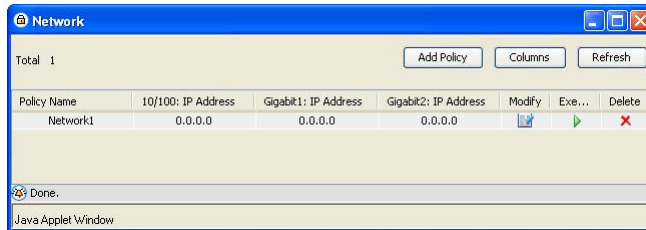


Figure 166. List of Network Policies

The columns in this window show selected settings for the listed policies. For information about changing the columns displayed, see [“Selecting the Columns Shown in a Policy Window” on page 220](#).

Creating a New Network Policy

A network policy is created so that you can define how the network interfaces of your Arrays are configured for connectivity to the network. The policy must offer the optimum network interface connectivity for all options (console, 10/100 Fast Ethernet, Gigabit 1 and Gigabit 2). See [Figure 167—“Network Interface Ports” on page 240](#).

To create a new network policy, click on the **Add Policy** button in the Network Policy window. When the Add Policy window appears, select **Copy from a chosen Array (recommended)** and choose a model Array, or select **Start from scratch**, as described in [“Adding a Policy” on page 219](#). Click OK.

The Network Settings window is divided into three primary areas:

- **10/100 (Fast Ethernet)**

The 10/100 (Fast Ethernet) interface provides wired network connectivity that runs at a maximum data transmission speed of 100 Mbps. This port is used for managing the Array and will only bridge management traffic, not data traffic.

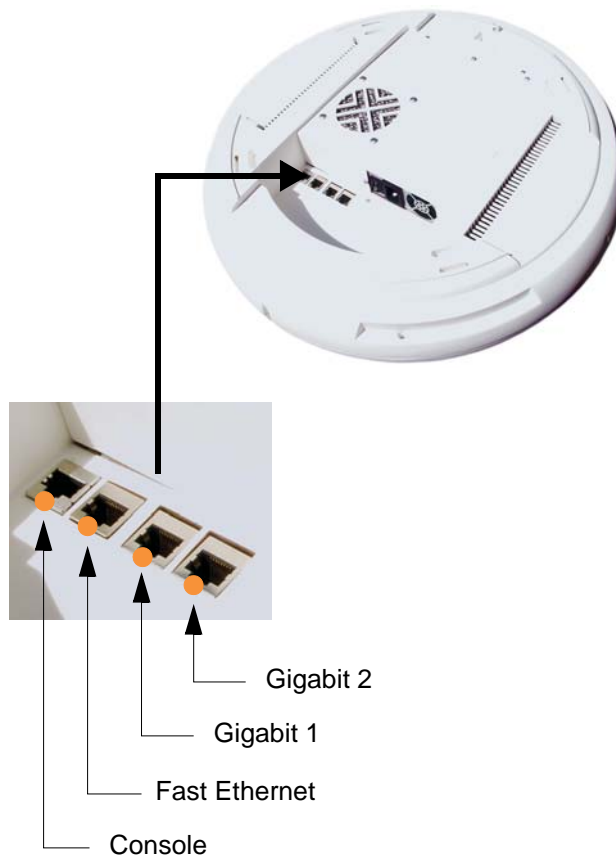


Figure 167. Network Interface Ports

- **Gigabit 1**

The Gigabit 1 interface is the primary port for both data and management traffic, providing wired network connectivity that runs at a maximum data transmission speed of 1000 Mbps. It is also backwards compatible with Fast Ethernet offering the slower data rate of 100 Mbps. If a single Ethernet connection is used, it must be connected to the Gigabit 1 port. If the Gigabit 1 interface fails, the Array automatically switches to Gigabit 2 for uninterrupted network connectivity. A Port Mode setting determines

how the two gigabit interfaces operate together in the normal situation when both ports are up.

- **Gigabit 2**

The Gigabit 2 interface mirrors the settings of the Gigabit 1 interface, including its ability to provide fail-over protection. For example, if the Gigabit 2 interface fails, the Array automatically switches to Gigabit 1 for uninterrupted network connectivity.

10/100 (Fast Ethernet)

This window contains fields for configuring the Fast Ethernet interface. The Fast Ethernet interface provides wired network connectivity that runs at a maximum data transmission speed of 100 Mbps. This port may only be used for managing the Array and will only bridge management traffic, not data traffic.

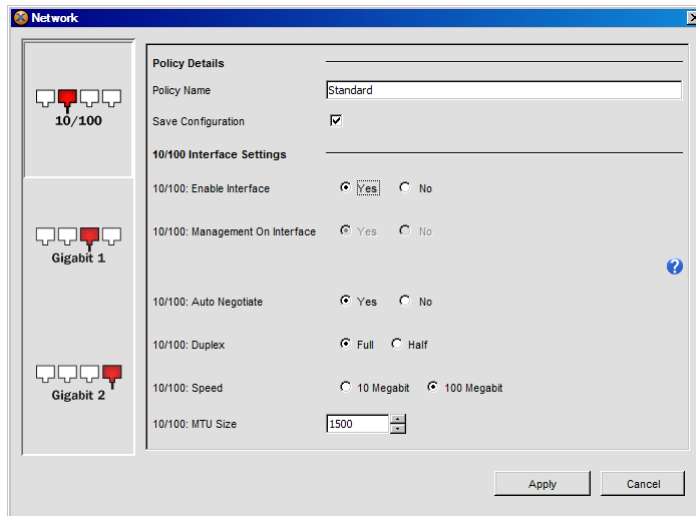


Figure 168. Network Settings (10/100 Fast Ethernet)

Policy Details

- **Policy Name**

Enter a meaningful name that describes this policy. If you are modifying an existing policy this field is grayed out (not editable). If you are using a

standard naming convention for all of your policies, the name you enter here should conform to that convention.

- **Save Configuration**

Check this box to ensure that any time this policy is applied to an Array, the Array will save the updated configuration information to its flash memory. If this box is left unchecked, then when this policy is applied to Arrays the configuration changes will need to be saved manually or else they will be lost when the Arrays are rebooted. Note that this checkbox does not actually apply the policy to any Arrays. To apply the policy, see **“Using Policy Windows” on page 218.**

10/100 Interface Settings



This policy cannot change IP address settings. This avoids problems with losing contact with the Array, and with creating duplicate address issues.

- **10/100: Enable Interface**

Choose **Yes** to enable the Fast Ethernet interface, or choose **No** to disable the interface. The default is Yes.

- **10/100: Management On Interface**

Array management is always enabled on this interface. You cannot disable management privileges.

- **10/100: Auto Negotiate**

This feature allows the Arrays to negotiate the best transmission rates automatically. Choose **Yes** to enable this feature, or choose **No** to disable this feature—the default is Yes. If you disable the Auto Negotiate feature, you must define the Duplex and Speed options manually.

- **10/100: Duplex**

Full-duplex refers to the transmission of data in two directions simultaneously (for example, a telephone is a full-duplex device because both parties can talk and be heard at the same time). In contrast, half-duplex only allows data transmission in one direction at a time. If the Auto-Negotiate feature is disabled, you must manually choose **Full** or **Half** duplex for your data transmission preference. The default is Full.

- **10/100: Speed**

If the Auto-Negotiate feature is disabled, you must manually choose the desired data transmission speed from the pull-down list, either **10 Megabit** or **100 Megabit**. The default is 100 Megabit.

- **10/100: MTU Size**

Specify the MTU (Maximum Transmission Unit) size. When you specify the MTU, you are defining—in bytes—the largest physical packet size that the network can transmit. Any messages larger than the MTU that you specify here are divided into smaller packets before being sent. The default is 1500 bytes.

After completing all of the desired fields in the 10/100 Fast Ethernet interface, either click on the **Apply** button to save this policy or click on one of the following buttons to configure more policy options:

- **Gigabit 1**

Configure the first Gigabit link.

- **Gigabit 2**

Configure the first Gigabit link.

Gigabit 1

This window contains fields for configuring the Gigabit 1 interface. The Gigabit 1 interface is the primary port for both data and management traffic, providing wired network connectivity that runs at a maximum data transmission speed of 1000 Mbps. It is also backwards compatible with Fast Ethernet, offering the slower data rate of 100 Mbps. If a single Ethernet connection is used, it must be connected to the Gigabit 1 port. If the Gigabit 1 interface fails and both ports are connected, the Array automatically switches to the **Gigabit 2** interface for uninterrupted network connectivity.

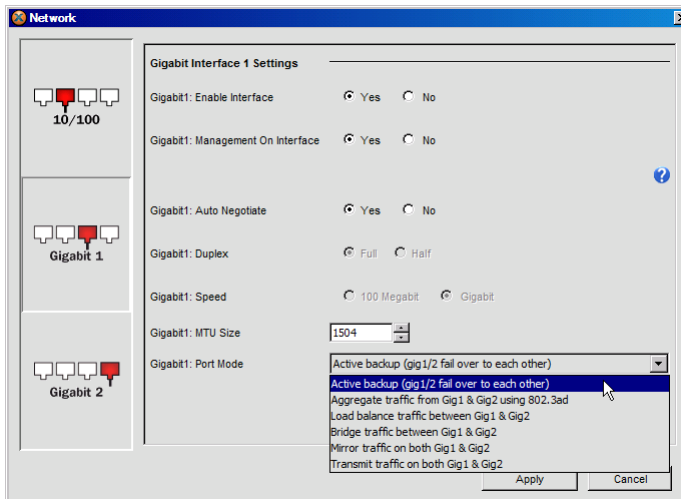


Figure 169. Network Settings (Gigabit 1)

Gigabit Interface 1 Settings



This policy cannot change IP address settings. This avoids problems with losing contact with the Array, and with creating duplicate address issues.

- **Gigabit 1: Enable Interface**

Choose **Yes** to enable the Gigabit 1 interface, or choose **No** to disable the interface. The default is Yes.

- **Gigabit 1: Management On Interface**

Choose **Yes** to enable Array management with this interface, or choose **No** to deny management privileges. The default is Yes.

- **Gigabit 1: Auto Negotiate**

This feature allows the Arrays to negotiate the best transmission rates automatically. Choose **Yes** to enable this feature, or choose **No** to disable this feature—the default is Yes. If you disable the Auto Negotiate feature, you must define the Duplex and Speed options manually.

- **Gigabit 1: Duplex**

Full-duplex refers to the transmission of data in two directions simultaneously (for example, a telephone is a full-duplex device because both parties can talk and be heard at the same time). In

contrast, half-duplex only allows data transmission in one direction at a time. If the Auto-Negotiate feature is disabled, you must manually choose **Full** or **Half** duplex for your data transmission preference. The default is Full.

- **Gigabit 1: Speed**

If the Auto-Negotiate feature is disabled, you must manually choose the desired data transmission speed from the pull-down list, either **100 Megabit** or **Gigabit**. The default is Gigabit.

- **Gigabit 1: MTU Size**

Specify the MTU (Maximum Transmission Unit) size. When you specify the MTU, you are defining—in bytes—the largest physical packet size that the network can transmit. Any messages larger than the MTU that you specify here are divided into smaller packets before being sent. The default is 1504 bytes.

- **Gigabit 1: Port Mode**

Specify how the two gigabit ports are to be use. The options are:

- **Active Backup (gig1/gig2 failover to each other)**—this is the default.
- **Aggregate Traffic from gig1 & gig2 using 802.3ad**
- **Bridge traffic between gig1 & gig2**
- **Transmit Traffic on both gig1 & gig2**
- **Load balance traffic between gig1 & gig2**
- **Mirror traffic on both gig1 & gig2**

For more information on these options, see the *Wi-Fi Array User's Guide*, part number 800-0006-001. For a detailed discussion, please see the *Xirrus Gigabit Ethernet Port Modes Application Note* in the [Xirrus Library](#).

After completing all of the desired fields in the Gigabit 1 interface, either click on the **Apply** button to save this policy or click on one of the following buttons to configure more policy options:

- **Gigabit 2**

Configure the second Gigabit link.

Gigabit 2

This window contains fields for viewing the Gigabit 2 interface settings. The Gigabit 2 interface mirrors the Gigabit 1 interface, including its ability to provide fail-over protection. For example, if the Gigabit 2 interface fails, the Array automatically switches to Gigabit 1 for uninterrupted network connectivity.

Gigabit Interface 2 Settings

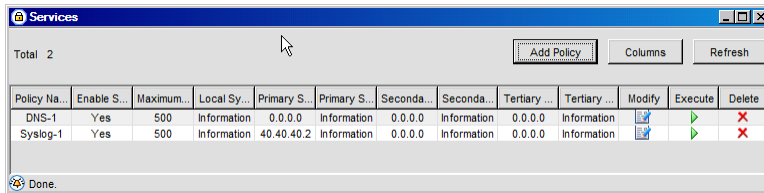
Because the configuration settings for the Gigabit 1 and Gigabit 2 network interfaces are the same, you cannot configure Gigabit 2 independently. Refer to [Gigabit Interface 1 Settings](#) to configure these options.

Saving Your Network Policy

When you have configured all of your network policy settings, click on the **Apply** button in the Network window to save the new policy.

Services

From the **Configuration>Policies** node in the tree, click on **Services** to display the Services window. This window contains a list of all service policies currently available, with tools to manage these policies.



Policy Na...	Enable S...	Maximum...	Local Sy...	Primary S...	Primary S...	Second...	Second...	Tertiary ...	Tertiary ...	Modify	Execute	Delete
DNS-1	Yes	500	Information	0.0.0.0	Information	0.0.0.0	Information	0.0.0.0	Information			
Syslog-1	Yes	500	Information	40.40.40.2	Information	0.0.0.0	Information	0.0.0.0	Information			

Figure 170. List of Services Policies

The columns in this window show selected settings for the listed policies. For information about changing the columns displayed, see [“Selecting the Columns Shown in a Policy Window” on page 220](#).

Creating a New Services Policy

A services policy is created so that you can configure all available servers at the same time, including enabling and disabling specific servers, assigning IP addresses for the servers, and establishing settings that are unique to each server. To create a new services policy, click on the **Add Policy** button in the Services Policy window. When the Add Policy window appears, select **Copy from a chosen Array (recommended)** and choose a model Array, or select **Start from scratch**, as described in [“Adding a Policy” on page 219](#). Click OK.

The Services window is displayed, which is divided into four primary areas:

- **DNS**

At least one DNS (Domain Name System) server should be set up for Arrays.

- **NTP**

The NTP (Network Time Protocol) server manages the time settings for your Arrays, including synchronizing the Array clocks with a universal clock from the NTP server. This ensures that System Log time-stamping is maintained across all units. Without an NTP server assigned (no

universal clock), each Array will use its own internal clock and stamp times accordingly, which may result in discrepancies.

- **NetFlow**

You may send NetFlow (IP flow) information to a designated collector, for later use and analysis.

- **System Log (Syslog)**

The System Log server processes messages based on network performance and usage. These messages include alerts, error messages, informational messages and notifications.

- **Standby**

The Standby Mode allows an Array to be designated as a backup unit that will only come online if its designated primary Array fails.

- **Wi-Fi Tags**

You may collect Wi-Fi Tag information on Arrays for later use and analysis.

DNS

This window contains a field for defining the name of the policy and fields for configuring the DNS server. At least one DNS server should be set up for Arrays.

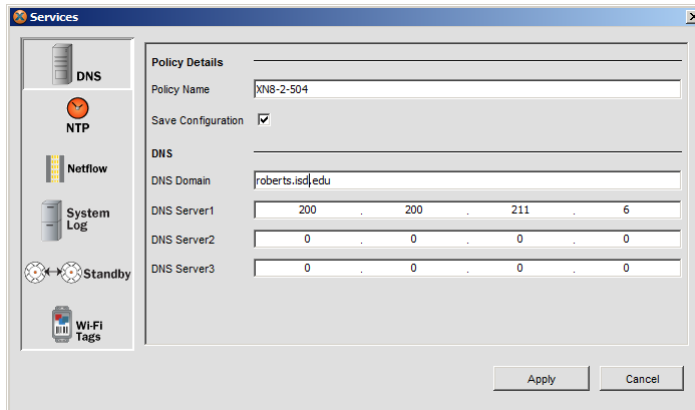


Figure 171. DNS Server Settings

Policy Details

- **Policy Name**

Enter a meaningful name that describes this policy. If you are modifying an existing policy this field is grayed out (not editable). If you are using a standard naming convention for all of your policies, the name you enter here should conform to that convention.

- **Save Configuration**

Check this box to ensure that any time this policy is applied to an Array, the Array will save the updated configuration information to its flash memory. If this box is left unchecked, then when this policy is applied to Arrays the configuration changes will need to be saved manually or else they will be lost when the Arrays are rebooted. Note that this checkbox does not actually apply the policy to any Arrays. To apply the policy, see [“Using Policy Windows” on page 218](#).

DNS Settings

- **DNS Domain**

Enter the DNS domain name for this server. DNS is used by the Arrays to lookup the names of various servers (for example, the System Log and NTP servers). You must specify a domain name when static IP addresses are used. This has the effect of appending the domain name to non-fully qualified address requests (for example, the NTP server host name configured as NTP1234 will become NTP1234.yourdomain.com).

- **DNS Server 1**

Enter the IP address of the primary DNS server.

- **DNS Server 2**

If you have a secondary DNS server available, enter the IP address of the this DNS server here.

- **DNS Server 3**

If you have a tertiary (third) DNS server available, enter the IP address of this DNS server here.

After completing all of the desired fields in the Services window for DNS, either click on the **Apply** button to save this policy or click on one of the following buttons to configure more service policy options:

- **NTP**
Configure the NTP server
- **NetFlow**
Configure the NetFlow collector.
- **System Log (Syslog)**
Configure the System Log server.
- **Standby**
Configure the standby Array.
- **Wi-Fi Tags**
You may collect Wi-Fi Tag information on Arrays for later use and analysis.

NTP

This window enables or disables an NTP server and has fields for configuring the server. The NTP server manages the time settings for your Arrays, including synchronizing the Array clocks with a universal clock from the NTP server. This ensures that System Log time-stamping is maintained across all units. Without an NTP server assigned (no universal clock), each Array will use its own internal clock and stamp times accordingly, which may result in discrepancies.

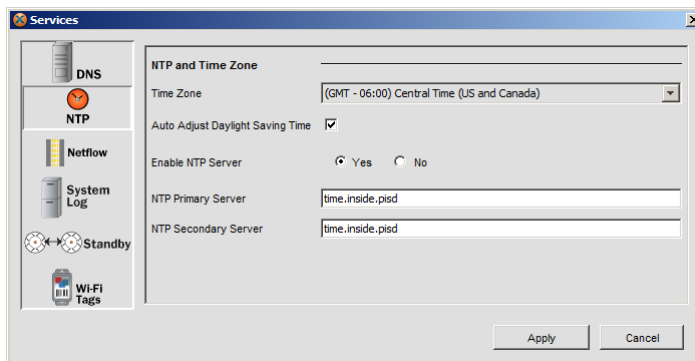


Figure 172. NTP Settings

NTP and Time Zone Settings

- **Time Zone**
Select the desired Time Zone from the drop-down list.
- **Auto Adjust Daylight Savings Time**
Enable this checkbox to allow the Array to automatically adjust the time for Daylight Savings Time.
- **Enable NTP Server**
Choose **Yes** to enable the NTP server, or choose **No** to disable the server.
- **NTP Primary Server**
If you enabled the NTP server, enter the IP address or DNS name of the server.
- **NTP Secondary Server**
If a secondary NTP server is available, enter the IP address or DNS name of the secondary NTP server.

After completing all of the desired fields in the Services window for NTP, either click on the **Apply** button to save this policy or click on one of the following buttons to configure more service policy options:

- **NetFlow**
Configure the NetFlow collector.
- **System Log (Syslog)**
Configure the System Log server.
- **Standby**
Configure the standby Array.
- **Wi-Fi Tags**
You may collect Wi-Fi Tag information on Arrays for later analysis.

NetFlow

This window allows you to enable or disable the sending of NetFlow information to a designated collector. NetFlow is a proprietary but open network protocol developed by Cisco Systems for collecting IP traffic information. When NetFlow is enabled on an Array, it will send IP flow information (traffic statistics) to the designated collector.

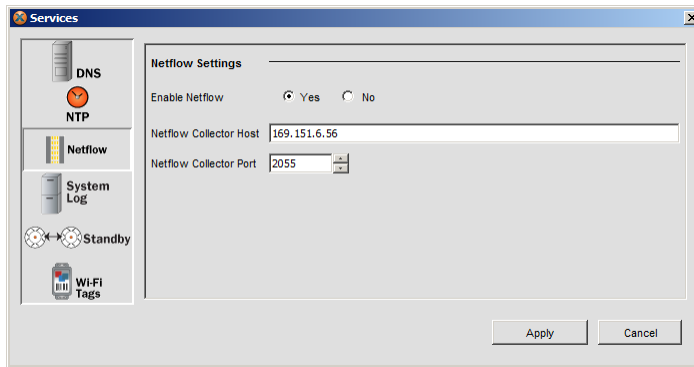


Figure 173. NetFlow Settings

NetFlow Settings

- **Enable NetFlow**
Choose **Yes** to enable the NetFlow functionality, or **No** to disable it.
- **NetFlow Collector Host**
If you enabled NetFlow, enter the IP address or hostname of the collector host.
- **NetFlow Collector Port**
If you enabled NetFlow, enter the port on the collector host to which to send data.

After completing all of the desired fields in the Services window for NetFlow, either click on the **Apply** button to save this policy or click on one of the following buttons to configure more service policy options:

- **System Log (Syslog)**
Configure the System Log server.

- **Standby**

Configure the standby Array.

- **Wi-Fi Tags**

You may collect Wi-Fi Tag information on Arrays for later analysis.

System Log (Syslog)

This window allows you to enable or disable a System Log server and contains fields for configuring the server. (Figure 174)

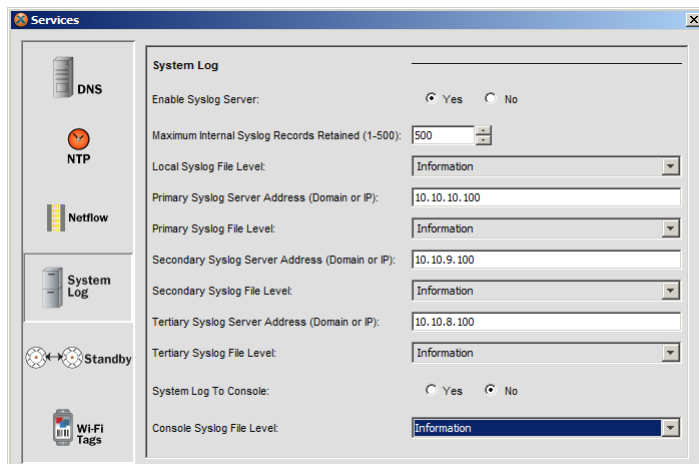


Figure 174. System Log Server Settings

The System Log server processes messages based on the network's performance and usage. These messages include alerts, error messages, informational messages and notifications.

System Log Server Settings

- **Enable System Log**

Choose **Yes** to enable the System Log server, or choose **No** to disable it. If you choose No, the remaining configuration fields for the System Log server are grayed out (not editable), and this procedure is finished.

- **Maximum Internal Syslog Records Retained (1-500):**
Enter a value in this field to define how many Syslog records are retained locally on the Array's internal Syslog file. The default is 500.
- **Local Syslog File Level**
Choose the level of System Log reporting for the Array's internal Syslog file from the pull-down list. Assigning a severity level informs the system to automatically log all messages in that level, and all messages above that level (messages below the assigned level are not logged). The debug level will significantly increase (almost double) the number of System Log messages that are returned and significantly degrade performance. The debug level should not be used for routine System Log reporting. Levels include:
 - Debug
 - Information
 - Notification
 - Warning
 - Error
 - Critical
 - Alerts
 - EmergencyThe default level is Information.
- **Primary Syslog Server Address (Domain or IP)**
If you enabled Syslog, enter the hostname or IP address of the primary Syslog server.
- **Primary Syslog File Level**
Choose the preferred level of Syslog reporting for the primary server. The default level is Information.
- **Secondary Syslog Server Address (Domain or IP)**
If you enabled Syslog, enter the hostname or IP address of an optional secondary Syslog server.

- **Secondary Syslog File Level**
Choose the preferred level of Syslog reporting for the secondary server. The default level is Information.
- **Tertiary Syslog Server Address (Domain or IP)**
If you enabled Syslog, enter the hostname or IP address of an optional tertiary Syslog server.
- **Tertiary Syslog File Level**
Choose the preferred level of Syslog reporting for the tertiary server. The default level is Information.
- **System Log to Console**
Choose **Yes** if you want System Log reporting directed to the Array's console interface, or choose **No** to suppress System Log messages to the console. Syslog messages will still be sent to servers as specified above.
- **Console Syslog File Level**
Choose the preferred level of Syslog reporting for the console. The default level is Information.

After completing all of the desired fields in the Services window for System Log, either click **Apply** or click one of the following to configure more services:

- **Standby**
Configure the standby Array.
- **Wi-Fi Tags**
You may collect Wi-Fi Tag information on Arrays for later use and analysis.

Standby

Standby Mode supports the Array-to-Array fail-over capability. When you enable Standby Mode, the Array functions as a backup unit, and it enables its radios if it detects that its designated primary Array has failed. The use of redundant Arrays to provide this fail-over capability allows Arrays to be used in mission-critical applications. In Standby Mode, an Array monitors beacons from the primary Array. When the primary has not been heard from for 40 seconds, the standby Array enables its radios until it detects that the primary Array has come back online. Standby Mode is off by default. Note that you must configure the standby

Array to match the configuration of the primary Array. The standby Array's configuration will not automatically synchronize.

This window allows you to enable or disable Standby Mode and specify the primary Array that is the target of the backup unit.

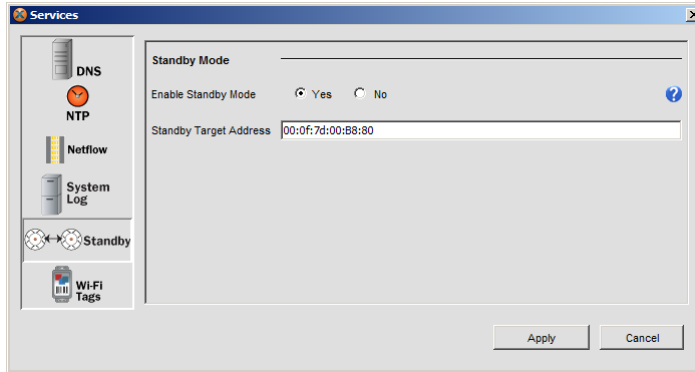


Figure 175. Standby Mode Settings

Standby Mode Settings

- **Enable Standby Mode**

Choose **Yes** to put an Array into Standby Mode, or choose **No** to allow the Array to operate normally. If you choose No, the remaining configuration fields are grayed out (not editable), and this procedure is finished.

- **Standby Target Address**

If you enabled Standby Mode, enter the base IAP MAC address of the target Array (i.e., the address of the primary Array that is being monitored and backed up by this Array). This address is the base address of the target Array's IAP MAC Range. To find this address, use the Web Management Interface on the primary Array ([“Connecting to an Array” on page 172](#)), and log in. Click **WDS**, and look for **This Array Address** at the bottom of the window. Alternatively, click **Array Info** and look for **IAP MAC Range**, then use the starting address of this range.

After completing all of the desired fields in the Services window for Standby, either click on the **Apply** button to save this policy or click on the following button to configure more service policy options:

- **Wi-Fi Tags**

You may collect Wi-Fi Tag information for later use and analysis.

Wi-Fi Tags

This window enables or disables Wi-Fi tag capabilities. When enabled, the Array listens for and collects information about Wi-Fi RFID tags sent on the designated channel. These tags are transmitted by specialized tag devices (for example, AeroScout Tags). A Wi-Fi tagging server (such as AeroScout) then queries the Array for a report on the tags that it has received. The Wi-Fi tagging server uses proprietary algorithms to determine locations for devices sending tag signals.

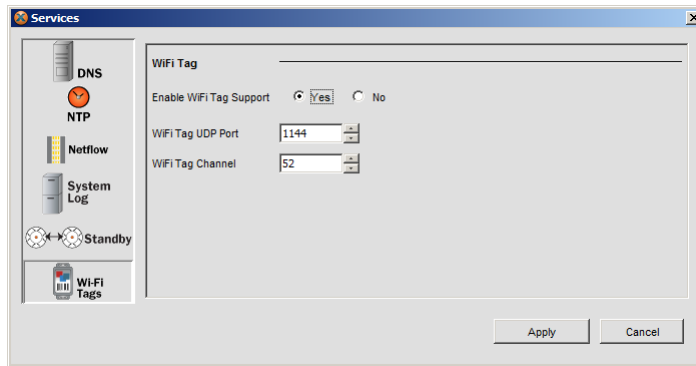


Figure 176. Wi-Fi Tag Settings

Wi-Fi Tag Settings

- **Enable Wi-Fi Tag**

Choose **Yes** to enable the Wi-Fi Tag functionality, or choose **No** to disable this feature.

- **Wi-Fi Tag UDP Port**

If you enabled Wi-Fi tagging, enter the port on the Array which the Wi-Fi tagging server will use to query the Array for tagging data. When queried, the Array will send back information on the tags it has observed. For each, the Array sends information such as the MAC address of the tag transmitting device, and the RSSI and noise floor observed.

- **Wi-Fi Tag Channel**

If you enabled Wi-Fi tagging, enter the 802.11 channel on which the Array will listen for tags. The tag devices must be set up to transmit on this channel.

Saving Your Services Policy

When you have configured all of your service policy settings, click on the **Apply** button in the Services window to save the new policy.

VLAN



For a complete discussion of implementing Voice over Wi-Fi on the Array, see the [Xirrus Voice over Wi-Fi Application Note](#) in the [Xirrus Library](#).

From the **Configuration>Policies** node in the tree, click **VLAN** to display the VLAN window. Use VLAN policies to add an Array to a VLAN.

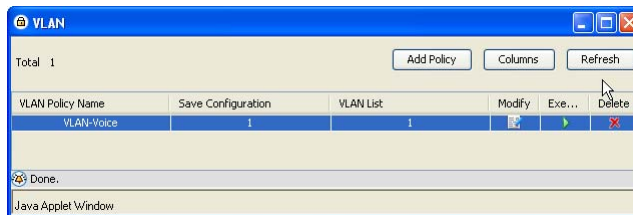


Figure 177. VLAN Policy List

The columns in this window show selected settings for the listed policies. For information about changing the columns displayed, see **“Selecting the Columns Shown in a Policy Window” on page 220**.



The Wi-Fi Array supports dynamic VLAN assignments specified by RADIUS policy settings. When RADIUS sends these assignments, the Array dynamically assigns wireless stations to VLANs as requested. VLAN tags on traffic are passed through the Array (i.e., VLAN tags are not stripped). Once a station has been dynamically moved to a new VLAN, it will be shown in the Stations window as a member of the new VLAN. (Figure 144 on page 203)

It is critical to configure all VLANs to be used on the Array, even those that will be dynamically assigned.

About Virtual Tunnels and VTun

Xirrus Arrays support Layer 2 tunneling with Virtual Tunnels. This allows an Array to use tunnels to transport traffic for one or more SSID-VLAN pairs onto a single destination network through the Layer 3 core network.

Virtual Tunnel Server (VTS)

Tunneling capability is provided by a Virtual Tunnel Server. You supply the server and deploy it in your network using open-source VTun software, available from vtun.sourceforge.net. For more information on setting up a server, please see *Wi-Fi Array User's Guide*, part number 800-0006-001. To enable an Array to use tunneling for a VLAN, enter the IP address, port and secret for your tunnel server as described in “[VLAN List Details](#)” on [page 263](#).

Creating a New VLAN Policy

A VLAN policy is created so that you can assign an Array to a VLAN. To create a new VLAN policy, click the **Add Policy** button in the VLAN Policy window. When the Add Policy window appears, select **Copy from a chosen Array (recommended)** and choose a model Array, or select **Start from scratch**, as described in “[Adding a Policy](#)” on [page 219](#). Click **OK**. The policy details window appears.

VLAN Name	VLAN number
VLAN2	2

Default Route Setting

VLAN ID: VLAN2

Native VLAN Setting

VLAN ID: [None]

Figure 178. VLAN Settings

Policy Details

- **Policy Name**

Enter a meaningful name that describes this policy. If you are modifying an existing policy this field is grayed out (not editable). If you are using a standard naming convention for all of your policies, the name you enter here should conform to that convention.

- **Save Configuration**

Check this box to ensure that any time this policy is applied to an Array, the Array will save the updated configuration information to its flash memory. If this box is left unchecked, then when this policy is applied to Arrays the configuration changes will need to be saved manually or else they will be lost when the Arrays are rebooted. Note that this checkbox does not actually apply the policy to any Arrays. To apply the policy, see [“Using Policy Windows” on page 218](#).

VLAN Setting

- **VLAN List**

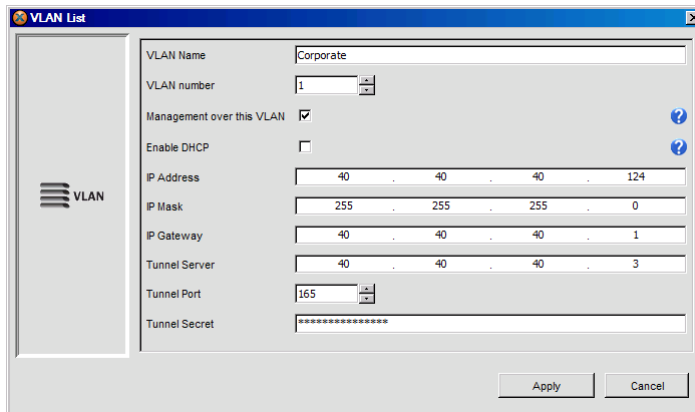




Figure 179. VLAN List Settings

A list of individual VLANs. VLANs may be added to the list by pressing the  button to the right of the list and filling in the fields shown below and described in [“VLAN List Details” on page 263](#); existing entries may

be edited by pressing the  button and deleted by pressing the  button.

Default Route Setting

You should set a default route VLAN if you will be managing the Array from a computer that is across a routed network. That is, if there is a router somewhere on the path between the management PC and the Array, the default route setting is necessary. Otherwise, this setting is not needed.

When a default route is specified, all management traffic (i.e., Array-generated traffic) such as NTP, syslogs, or traps will go out tagged with the default route VLAN tag. If no default route is defined, then all management traffic will exit the Array untagged.

- **VLAN ID**

Select a VLAN from the drop-down list to be the default route VLAN. The VLAN address must have been completely configured - either use DHCP or set the IP address, IP (subnetwork) mask, and gateway.

Native VLAN Setting

The native VLAN is required for proper interaction between the Array and a port operating in native mode. For example, the Array may be connected to a port on a Cisco switch that is configured for native mode. When operating in native mode, a switch port strips all VLAN tags and sends out untagged traffic. The Array will assign all untagged incoming traffic to the designated native VLAN. The native VLAN provides the Array with an internal mechanism that allows it to handle this untagged traffic.

In particular, setting a native VLAN allows management of the Array across a path that includes a switch port operating in native mode.

- **VLAN ID**

Select a VLAN from the drop-down list to be the native VLAN. The VLAN must have been completely configured - either use DHCP or set the IP address, IP (subnetwork) mask, and gateway.

You may select any VLAN from the list as the native VLAN, even if it is also used for other purposes.

VLAN List Details

- **VLAN Name**
Enter the name of the VLAN that you wish to create.
- **VLAN Number**
Enter the unique number that is assigned to your VLAN.
- **Management over this VLAN**
Select the check box to allow the Array to be managed over the VLAN. The VLAN address must also be configured.
- **Enable DHCP**
Enable this setting if you want the Array to get its IP address from a DHCP server.
- **IP Address**
Enter an IP address only you are using a static IP address.
- **IP Mask**
Enter the IP mask used by your network only if you are using a static IP address.
- **IP Gateway**
Enter the IP address of the gateway used by your network, only if you are using a static IP address.
- **Tunnel Server**
If this VLAN is to be tunneled, enter the IP address or host name of the tunnel server that will perform the tunneling. For more information on virtual tunnels, please see [“About Virtual Tunnels and VTun” on page 259](#).
- **Tunnel Port**
If this VLAN is to be tunneled, enter the port number of the tunnel server.
- **Tunnel Secret**
Enter the password expected by the tunnel server.

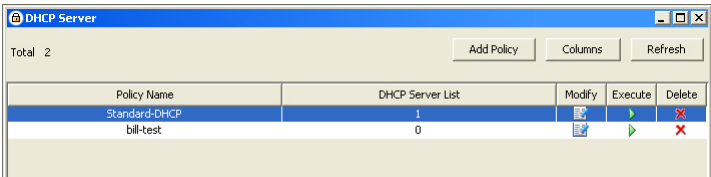
When you have completed the settings for this VLAN, click the **Apply** button to save the VLAN.

Saving Your VLAN Policy

When you have configured all of your VLAN policy settings, click on the **Apply** button in the VLAN window to save the new policy.

DHCP Server

From the **Configuration>Policies** node in the tree, click on **DHCP Server** to display the DHCP Server window. This window contains a list of all DHCP Server policies currently available, with tools to manage these policies.



The screenshot shows a window titled "DHCP Server" with a toolbar containing "Add Policy", "Columns", and "Refresh" buttons. Below the toolbar, it says "Total 2". A table lists the policies:

Policy Name	DHCP Server List	Modify	Execute	Delete
Standard-DHCP	1			
bill-test	0			

Figure 180. List of DHCP Server Policies

The columns in this window show selected settings for the listed policies. For information about changing the columns displayed, see **“Selecting the Columns Shown in a Policy Window” on page 220**.

A DHCP policy is created so that you can configure DHCP servers. The DHCP (Dynamic Host Configuration Protocol) server allows the Arrays to provide wireless clients with IP addresses and other networking information. The DHCP server will not provide DHCP services to the wired side of the network. To create a new server policy, click on the **Add Policy** button in the DHCP Server policy window. When the Add Policy window appears, select **Copy from a chosen Array (recommended)** and choose a model Array, or select **Start from scratch**, as described in **“Adding a Policy” on page 219**. Click **OK**. The policy details window appears.

DHCP Server Policy

This window contains fields for configuring pools of IP addresses (DHCP pools) that the DHCP server may assign to clients. The DHCP server allows the Arrays to provide wireless clients with IP addresses and other networking information. The DHCP server will not provide DHCP services to the wired side of the network. If you enable a DHCP server, you need to define the DHCP lease time (default and maximum) and establish the IP address ranges (DHCP pools) that the DHCP server can use.

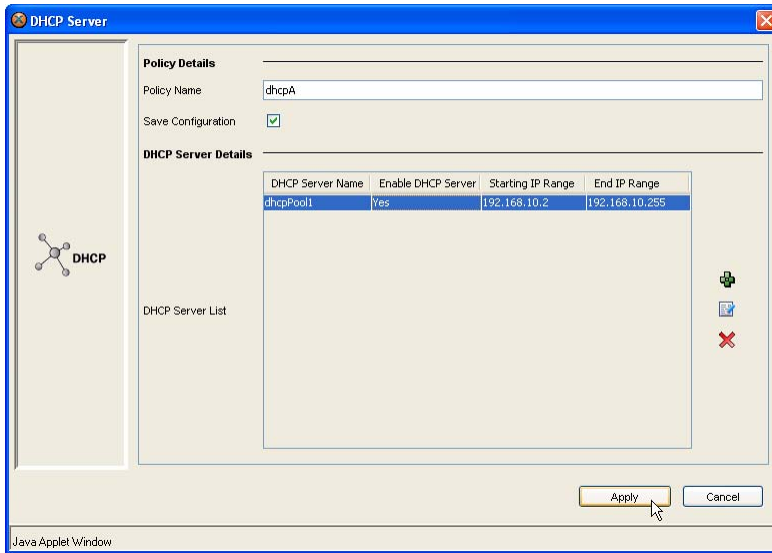


Figure 181. DHCP Server Settings

Policy Details

- **Policy Name**




Enter a meaningful name that describes this policy. If you are modifying an existing policy this field is grayed out (not editable). If you are using a standard naming convention for all of your policies, the name you enter here should conform to that convention.

- **Save Configuration**

Check this box to ensure that any time this policy is applied to an Array, the Array will save the updated configuration information to its flash memory. If this box is left unchecked, then when this policy is applied to Arrays the configuration changes will need to be saved manually or else they will be lost when the Arrays are rebooted. Note that this checkbox does not actually apply the policy to any Arrays. To apply the policy, see [“Using Policy Windows” on page 218](#).

DHCP Server Policy Details

- **DHCP Server List**

This shows a list of DHCP pools (a range of IP addresses that may be distributed by the server). A DHCP pool may be added to the list by pressing the  button to the right of the list and filling in the fields shown below and described in **DHCP Pool** below; existing pools may be edited by pressing the  button and deleted by pressing the  button. Multiple pools may be defined for the same server.

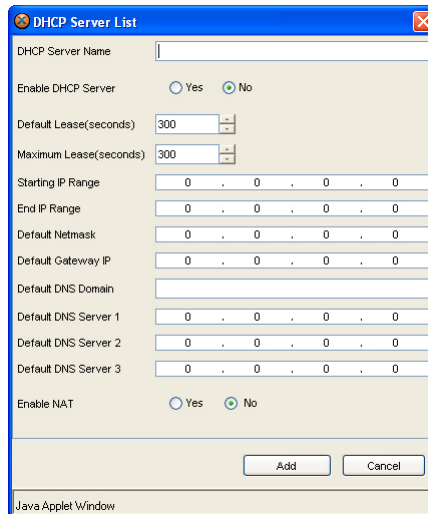


Figure 182. DHCP List Settings

DHCP Pool

- **DHCP Server Name**

The name associated with this DHCP pool.

- **Enable DHCP Server**

Choose **Yes** to enable the DHCP server, or choose **No** to disable the server. If you choose No, the remaining configuration fields for the DHCP server are grayed out (not editable), and this procedure is finished.

- **Default Lease**

Enter a value in this field to define the default DHCP lease time (in seconds), or increment/decrement the time using the UP and DOWN arrows. The default is 300 seconds.

When DHCP is used, one of the most important decisions to be made is the lease length policy—how long the administrator wants client leases to last. The best lease length interval depends on the network, the DHCP server, and the clients it serves. The lease time is a trade-off between network stability and allocation efficiency.

The primary benefit of using long lease times is that the addresses of devices are relatively stable, because a device doesn't have to worry about its IP address changing all the time—and neither does its user. The main drawback of using a long lease time is that it substantially increases the amount of time that an IP address tied up before it can be reused (once it is no longer needed).

Most network administrators prefer to use a short lease time. This forces the client to continually renew the lease as long as it needs it. When the client stops requesting the IP address, the address is quickly put back into the pool—a more efficient method in environments where the number of addresses is limited and must be conserved. The drawback is the opposite of the benefit of a long lease time, with constantly-changing IP addresses.

- **Maximum Lease**

Enter a value in this field to define the maximum allowable DHCP lease time (in seconds), or increment/decrement the time using the UP and DOWN arrows. The default is 300 seconds.

- **Starting IP Range**

Enter an IP address to define the start of the IP range for this DHCP pool that will be used by the DHCP server.

- **End IP Range**

Enter an IP address to define the end of the IP range for this DHCP pool that will be used by the DHCP server. For this pool, the DHCP server will only use IP addresses that fall between the start and end range that you define.

- **Default Netmask**
Enter the subnet mask IP address for the DHCP server.
- **Default Gateway IP**
If necessary, enter the IP address of the gateway.
- **Default DNS Domain**
Enter the DNS domain name. See also, [“DNS Settings” on page 249](#).
- **Default DNS Server 1 (and DNS Server 2 and DNS Server 3)**
Enter the IP address of the primary DNS server, secondary DNS server and tertiary DNS server. See also, [“DNS Settings” on page 249](#).
- **Enable NAT**
NAT (Network Address Translation) translates between the internal IP addresses assigned to stations by the Array’s DHCP server and global (external) IP addresses. NAT reduces the number of global IP addresses that a company needs and allows the company use a single IP address externally. Choose **Yes** to enable NAT for this IP address pool, or choose **No** to disable it.

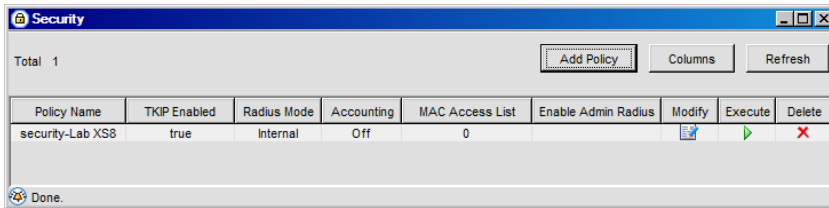
Click the **Add** button to add this DHCP pool to the policy and return to the policy window.

Saving Your DHCP Server Policy

When you have configured all of your DHCP policy settings, click on the **Apply** button in the DHCP Server window to save the new policy.

Security

From the **Configuration>Policies** node in the tree, click on **Security** to display the Security window. This window contains a list of all security policies currently available, with tools to manage these policies.






Policy Name	TKIP Enabled	Radius Mode	Accounting	MAC Access List	Enable Admin Radius	Modify	Execute	Delete
security-Lab XS8	true	Internal	Off	0				

Figure 183. List of Security Policies

The columns in this window show selected settings for the listed policies. For information about changing the columns displayed, see [“Selecting the Columns Shown in a Policy Window” on page 220](#).

Creating A New Security Policy

A security policy is created so that you can define how your Arrays control administrator and user access and prevent intrusion into the network by unauthorized users. To create a new security policy, click on the **Add Policy** button in the Security Policy window. When the Add Policy window appears, select **Copy from a chosen Array (recommended)** and choose a model Array, or select **Start from scratch**, as described in [“Adding a Policy” on page 219](#). Click **OK**.

The policy details window is displayed, which is divided into four primary areas:

- **Security**

The latest and most effective wireless security standards, including WPA with 802.11i AES (Advanced Encryption Standard) are implemented with each Wi-Fi Array using this policy. This area of the policy defines the name of the policy, allows you to enable or disable WPA and WEP, and define the parameters for a WPA or WEP enabled policy.

- **RADIUS**

The use of an embedded RADIUS server (or 802.1X with an external RADIUS server) ensures user authentication—multiple Arrays can authenticate to XMS ensuring only authorized Arrays become part of the wireless network. This area of the policy allows you to define either internal (embedded) or external RADIUS accounting, set up the server parameters for an external RADIUS server, or establish a list of users for the internal RADIUS server.

- **MAC Access List**

An access control list, based on MAC address, can be assigned to restrict user access. This area of the policy allows you to set up the type of MAC access control list (disable, allow or deny), and add or remove users from the list. You can also view the list and its contents without making changes

- **Admin RADIUS**

The Admin RADIUS policy allows you to set up authentication of Array administrators via RADIUS, rather than using the local administrator accounts on Arrays.

Security

This window contains a field for defining the name of the policy and fields for configuring the WPA and WEP information.

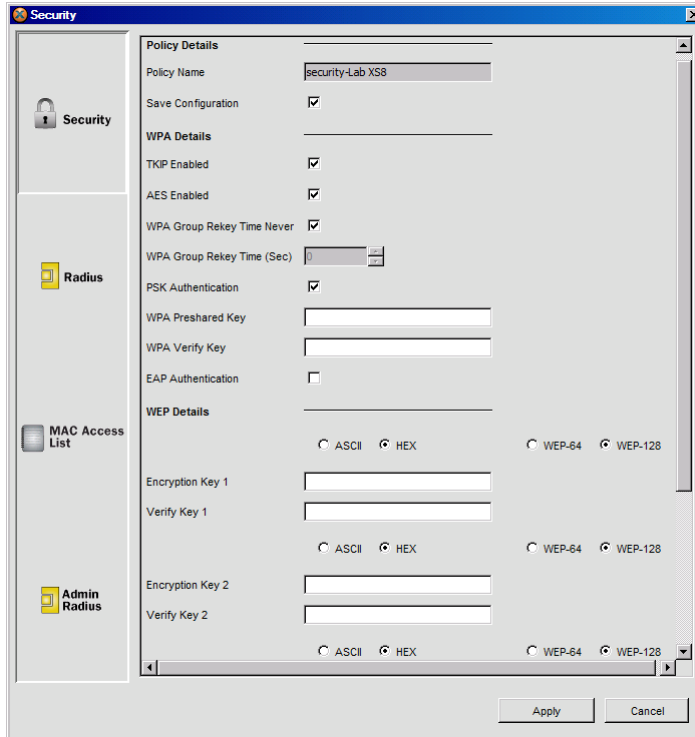


Figure 184. Security Settings

Policy Details

- **Policy Name**

Enter a meaningful name that describes this policy. If you are modifying an existing policy this field is grayed out (not editable). If you are using a standard naming convention for all of your policies, the name you enter here should conform to that convention.

- **Save Configuration**

Check this box to ensure that any time this policy is applied to an Array, the Array will save the updated configuration information to its flash memory. If this box is left unchecked, then when this policy is applied to Arrays the configuration changes will need to be saved manually or else they will be lost when the Arrays are rebooted. Note that this checkbox does not actually apply the policy to any Arrays. To apply the policy, see [“Using Policy Windows” on page 218](#).

WPA Details

- **TKIP Enabled**

Check this box to enable the TKIP (Temporal Key Integrity Protocol) encryption standard. TKIP provides improved data encryption by scrambling security keys using a hashing algorithm and, by adding an integrity checking feature, ensures that the encryption keys haven’t been tampered with. Uncheck this box if you want to disable TKIP.

- **AES Enabled**

Check this box to enable AES (Advanced Encryption Standard). AES is a data encryption scheme that uses three different key sizes (128 bit, 192 bit, and 256 bit). AES is the strongest encryption standard and is used by government agencies; however, old legacy hardware may not be capable of supporting the AES mode (it probably won’t work on older wireless clients). Because AES is the strongest encryption standard currently available, it is highly recommended for Enterprise networks. Uncheck this box if you want to disable AES.

- **WPA Group Rekey Time Never and WPA Group Rekey Time (Sec)**

Enter a value in **WPA Group Rekey Time (Sec)** to define the WPA group rekey time (in seconds), or increment/decrement the time using the UP and DOWN arrows. The value you enter determines the elapsed time before the system uses an alternative security key. If you wish to prevent rekeying, check the **Never** checkbox.

- **PSK Authentication**

Check this box to enable PSK (Pre-Shared Key) authentication. With PSK enabled, users must manually enter a key (passphrase) on the client side

of the wireless network that matches the key stored on XMS and assigned to an Array or group of Arrays. Only enable PSK for smaller networks when a RADIUS server is unavailable. Uncheck this box if you want to disable PSK authentication.

- **WPA Preshared Key**

If you enabled PSK, enter a passphrase here. Choose a strong passphrase containing between 8 and 63 characters (20 is preferred). Always use a combination of letters, numbers and special characters. Never use English words separated by spaces.

- **WPA Verify Key**

Retype your WPA Preshared Key in this field to verify that you typed it correctly.

- **EAP Authentication**

Check this box to enable EAP ((Extensible Authentication Protocol). An external RADIUS server must be defined if you want to make use of EAP authentication. An external RADIUS server offers more functionality and security, and is recommended for large deployments. When using this method, user names and passwords must be entered into an LDAP server for user authentication. Uncheck this box if you want to disable EAP authentication.

You must enable either WPA or WEP encryption (next section) for an SSID to ensure that you have an acceptable level of security for your network. The encryption type is selected per SSID (see **Security Type** in “**SSID List Details**” on [page 289](#)). Xirrus recommends either WPA or WPA2. The only time that you might create a policy with all security options disabled is if the clients assigned to that policy are required to use a VPN connection through a secure SSH utility, like **PuTTY**.

WEP Details

If WEP is enabled, enter the following information for up to four encryption keys:

- **Mode: ASCII / Hex**

Choose the key mode (either ASCII or Hex).

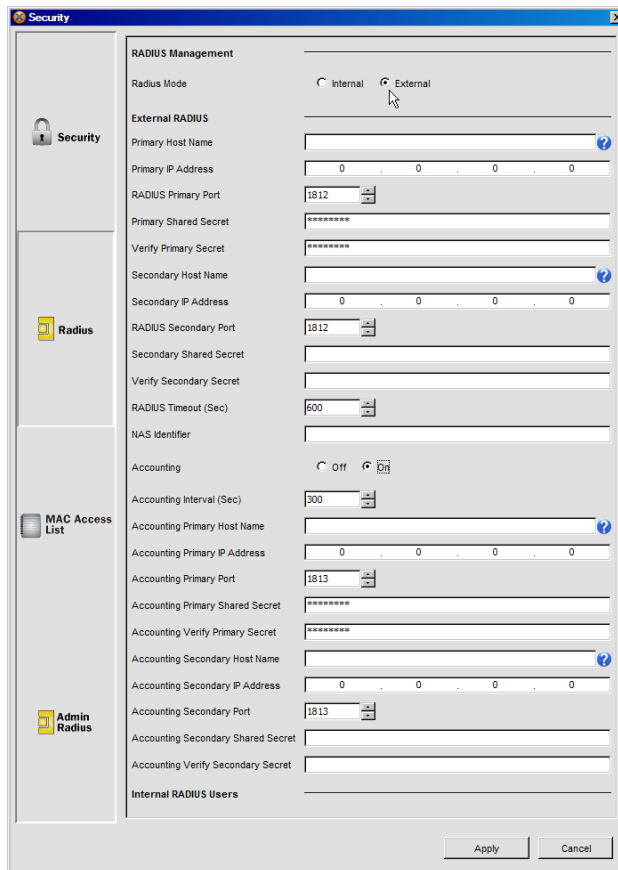
- **Length: WEP-64 / WEP-128**
Choose the desired key length (either 64 or 128).
- **Encryption Key**
Enter an encryption key of the length and mode selected above.
 - WEP-64: 10 hex/5 ASCII characters for 40 bits.
 - WEP-128: 26 hex/13 ASCII characters for 104 bits.Hexadecimal characters are defined as ABCDEF and 0-9. For ASCII mode, do not use special characters.
- **Verify Key**
Retype your Encryption Key in this field to verify that you typed it correctly.
- (Optional) Repeat the instructions above to create and verify up to 4 WEP encryption keys in the **Encryption Key 2, 3, and 4** sections.
- **Default Key**
From the pull-down list, choose which of the configured keys you want to assign as the default key (either Key 1, Key 2, Key 3, or Key 4).

After completing all of the desired fields in the Security window, either click on the **Apply** button to save this policy or click on one of the following buttons to configure more security policy options:

- **RADIUS**
Configure an internal or external RADIUS server. Xirrus recommends using an external RADIUS server, if available.
- **MAC Access List**
Configure an access control list based on MAC addresses.
- **Admin RADIUS**
Set up Array administrator authentication via external RADIUS servers.

RADIUS

This window allows you to specify if the RADIUS server is internal or external. If you specify an internal RADIUS server, you can create a user access list with passwords tied to an SSID. If you specify an external RADIUS server, you must define parameters for the primary server (and secondary server, if available) with any shared secrets. (Figure 185)



Security

RADIUS Management

Radius Mode: ☐ Internal ☒ External

External RADIUS

Primary Host Name:

Primary IP Address:

RADIUS Primary Port:

Primary Shared Secret:

Verify Primary Secret:

Secondary Host Name:

Secondary IP Address:

RADIUS Secondary Port:

Secondary Shared Secret:

Verify Secondary Secret:

RADIUS Timeout (Sec):

NAS Identifier:

Accounting

☐ Off ☒ On

Accounting Interval (Sec):

Accounting Primary Host Name:

Accounting Primary IP Address:

Accounting Primary Port:

Accounting Primary Shared Secret:

Accounting Verify Primary Secret:

Accounting Secondary Host Name:

Accounting Secondary IP Address:

Accounting Secondary Port:

Accounting Secondary Shared Secret:

Accounting Verify Secondary Secret:

Internal RADIUS Users

Apply Cancel

Figure 185. RADIUS Management

RADIUS Management Details

- **Internal or External**

Choose either Internal or External for the type of RADIUS server. If you choose Internal, the RADIUS server will only authenticate wireless clients that want to associate to Arrays that are using this policy if they are included in the **Internal RADIUS Users Details** list—useful if an external RADIUS server is not available. If an external RADIUS server is available choose External to take advantage of the added user authentication functionality that comes with 802.1X technology.

External RADIUS Details

The fields in this section only become available if you chose External when defining the type of RADIUS server (otherwise they are grayed out).



*You may specify the RADIUS servers (including accounting servers) by either IP address or host name. To prevent confusion, we recommend that you specify one or the other, but not both. **If you do enter both, only the IP address will be used.** The host name will only be sent to Arrays running ArrayOS Release 3.5 or above.*

- **Primary Host Name**

Enter the hostname of the primary RADIUS server. If you enter an IP address as well, the IP address has precedence and the host name will be ignored.

- **Primary IP Address**

Enter the IP address of the primary RADIUS server.

- **RADIUS Primary Port**

Enter the port number for the primary RADIUS server, or increment/decrement the number using the UP and DOWN arrows.

- **Primary Shared Secret**

Enter the primary shared secret. This is the secret that is shared between the user and the external RADIUS server. Users can only be authenticated if they are using the same shared secret.

- **Verify Primary Secret**
Retype your Primary Secret in this field to verify that you typed it correctly.
- (Optional) Repeat the instructions in the previous four bullets to define a secondary RADIUS server, if available. If the primary server goes off-line, the Array will “failover” to this secondary server (defined here).
- **RADIUS Timeout**
Enter the maximum idle time (in seconds) before the RADIUS session times out. The default is 600 seconds.
- **NAS Identifier**
From the point of view of the RADIUS server, the Array functions as a client, also called a network access server (NAS). Enter the NAS Identifier that the RADIUS servers expect the Array to use.
- **Accounting:** If you would like the Array to send RADIUS Start, Stop, and Interim records to a RADIUS accounting server, click the **On** button. The following fields appear.
 - **Accounting Interval (seconds):** Specify how often Interim records are to be sent to the server.
 - **Accounting Primary Host Name:** Enter the hostname of the primary RADIUS accounting server. If you enter an IP address as well, the IP address has precedence and the host name will be ignored.
 - **Accounting Primary IP Address:** Enter the IP address of the primary RADIUS accounting server that you intend to use.
 - **Accounting Primary Port Number:** Enter the port number of the primary RADIUS accounting server. The default is 1813.
 - **Accounting Primary Shared Secret / Verify Secret:** Enter the shared secret that the primary RADIUS accounting server will be using, then re-enter the shared secret to verify that you typed it correctly.
 - **Accounting Secondary Host Name:** Enter the hostname of the secondary RADIUS accounting server. If the primary server goes off-line, the Array will “failover” to this secondary server (defined here).

If you enter an IP address as well, the IP address has precedence and the host name will be ignored.

- **Accounting Secondary IP Address** (optional): If desired, enter a secondary IP address for an alternative RADIUS accounting server.
- **Accounting Secondary Port Number**: If using a secondary accounting server, enter its port number. The default is 1813.
- **Accounting Secondary Shared Secret / Verify Secret**: If using a secondary accounting server, enter the shared secret that it will be using, then re-enter the shared secret to verify that you typed it correctly.

If you do not want to set up a list of users for an internal RADIUS server, and after completing all of the desired fields for the external RADIUS server, either click on the **Apply** button to save this policy or click on one of the following buttons to configure more security policy options:

- **MAC Access List**
Configure an access control list based on MAC addresses.
- **Admin RADIUS**
Set up Array administrator authentication via external RADIUS servers.

Internal RADIUS Users Details

This section is normally only applicable if you chose **Internal** when defining the type of RADIUS server. However, you can still set up a list of users for an internal RADIUS server and use this option as a backup if your external server becomes unavailable. Internal RADIUS server users are defined by their name, password and associated SSID.

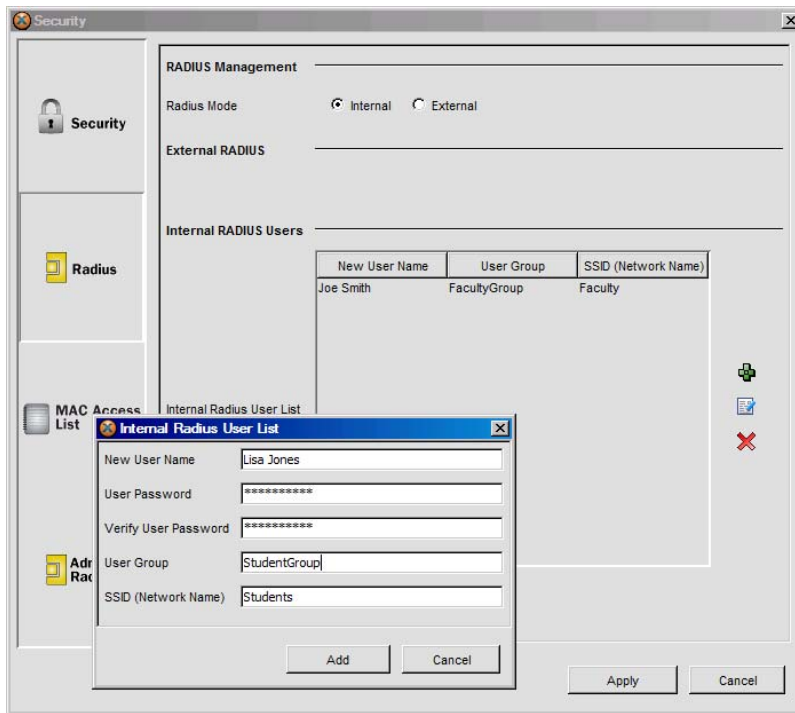



Figure 186. Adding Internal RADIUS Users

To create a new user, click on the  button to display the Internal RADIUS User List window. (Figure 186)

- **New User Name**
Enter the name of the new user.
- **User Password**
Enter a unique password for the new user.
- **Verify User Password**
Retype the user password in this field to verify that you typed it correctly.
- **User Group**
If you want to make this user a member of a previously defined user group, enter the name of the group. This will apply all of the user group's settings on the Array to the user.

- **SSID (Network Name)**

Enter an SSID for this user. This will be the only SSID that the user can associate with.

When you have finished inputting data for the new user, click on the **Add** button to add this user to the list and close the Internal RADIUS User List window.

After completing all of the desired fields in the RADIUS window, either click on the **Apply** button to save this policy or click on one of the following buttons to configure more security policy options:

- **MAC Access List**

Configure an access control list based on MAC addresses.

- **Admin RADIUS**

Set up Array administrator authentication via external RADIUS servers.

MAC Access List

This window allows you to create an access control list for users based on the MAC addresses of the clients they are using. The list can be defined as an **Allow List**, which PERMITS access to the network only to the clients who are included in the list. The list can also be defined as a **Deny List**, which PREVENTS access to the network by any client included in the list.

Deny lists are generally easier to maintain because you can add users to the list arbitrarily—either because you don't recognize the MAC address, or because you do recognize the MAC address and you don't trust the client. With an Allow List you must maintain accurate records of your users and ensure that they appear in the list, otherwise you run the risk of denying access to trusted users.

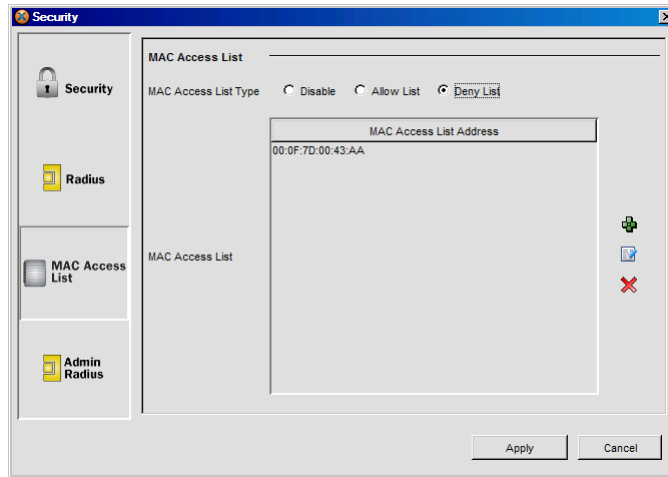



Figure 187. MAC Access List

MAC Access List Type

Choose the type of access control list you want to create, either an **Allow List** or a **Deny List**. You also have the option of choosing **Disable**, which will disable this functionality and render any client MAC addresses in the list redundant. If you disable this feature, you can always enable it again at a later time.

Creating control lists, whether MAC access lists, rogue AP lists, or any other type of control list is always beneficial even if you do not intend to make use of the list immediately—control lists can be used as a backup at anytime, and the lists should be kept up-to-date whenever possible.

To add a new MAC address to the access control list, click on the  button to display the MAC Access List Address window.

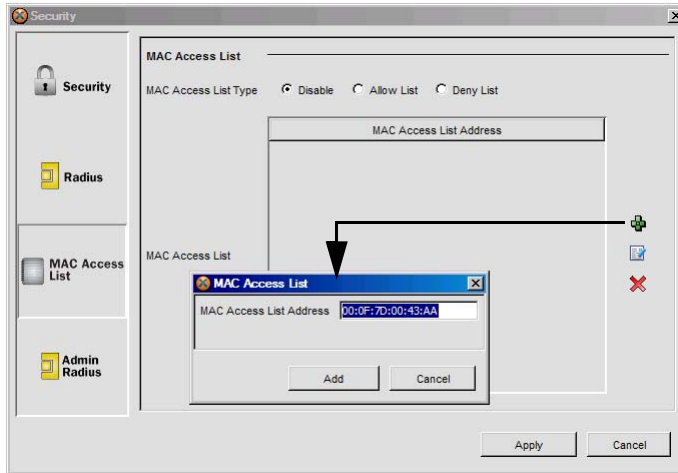


Figure 188. Adding a MAC Address to the MAC Access List

- **MAC Access List Address**

Enter the MAC address, then click **Add**. You are returned to the MAC Access List window where the new address appears in the list.

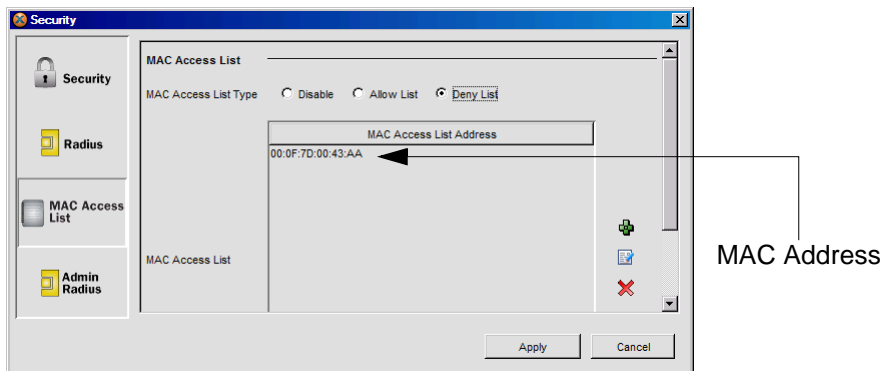


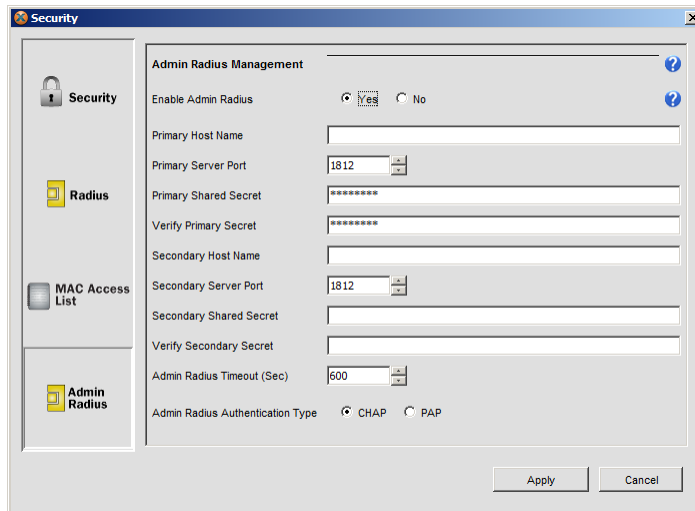
Figure 189. MAC Access List

When you have finished adding all of your MAC addresses, either click on the **Apply** button to save this policy or click on the **Admin RADIUS** button to configure more security policy options.

Admin RADIUS

The Admin RADIUS policy (**Figure 190**) allows you to set up authentication of network administrators via RADIUS, rather than using the local administrator accounts on Arrays. Using RADIUS to control administrator accounts for logging in to Arrays has these benefits:

- Centralized control of administrator accounts.
- Less effort—you don't have to set up user names and passwords on each Array; just enter them once on the RADIUS server and then all of the Arrays can pull from the RADIUS server.
- Enforced policies—you may set password rules (e.g., passwords must contain at least one number and be at least 12 characters in length), and you may set expiration times for passwords.



The screenshot shows the 'Security' management window with a sidebar containing 'Security', 'Radius', 'MAC Access List', and 'Admin Radius'. The 'Admin Radius' option is selected. The main panel is titled 'Admin Radius Management' and contains the following fields and controls:

- Enable Admin Radius:** Radio buttons for 'Yes' (selected) and 'No'.
- Primary Host Name:** A text input field.
- Primary Server Port:** A numeric input field with the value '1812'.
- Primary Shared Secret:** A text input field with masked characters (asterisks).
- Verify Primary Secret:** A text input field with masked characters (asterisks).
- Secondary Host Name:** A text input field.
- Secondary Server Port:** A numeric input field with the value '1812'.
- Secondary Shared Secret:** A text input field with masked characters (asterisks).
- Verify Secondary Secret:** A text input field with masked characters (asterisks).
- Admin Radius Timeout (Sec):** A numeric input field with the value '600'.
- Admin Radius Authentication Type:** Radio buttons for 'CHAP' (selected) and 'PAP'.

At the bottom right of the window are 'Apply' and 'Cancel' buttons.

Figure 190. Admin RADIUS Management

Admin RADIUS settings override any local administrator accounts configured on an Array. If you enable Admin RADIUS on an Array, all administrator authentication is done via the configured RADIUS servers. The only exception to this is when an administrator is connected via an Array's Console port (using CLI). In that case, the Array will authenticate administrators using accounts configured on the **Management Control—Admin** window first, and then use the RADIUS servers. This provides a safety net to ensure that administrators are not completely locked out of an Array if the RADIUS server is down.

Setting Up Admin Accounts on the RADIUS Server

Permissions for RADIUS administrator accounts are controlled by the RADIUS **Service-Type** attribute (Attribute 6). To grant read-write permission, configure the RADIUS server to send back the Service-Type attribute with a value of **Administrative** (value=6). To grant read-only permission, the RADIUS server should send the Service-Type attribute with a value of **NAS Prompt** (value=7).

When configuring administrator accounts on the RADIUS server, you must observe the same restrictions for length and legal characters as when creating these accounts on the Array using the **Management Control—Admin** window: the user name and password must be between 5 and 50 characters, inclusive.

Admin RADIUS Setting Details

- **Enable Admin RADIUS**

Click **Yes** to enable the use of RADIUS to authenticate administrators logging in to the Array. You will need to specify the RADIUS server(s) to be used.

The following fields only become available if you chose **Yes** to enable admin RADIUS (otherwise they are grayed out).

- **Primary Host Name**

Enter the host name or IP address of the primary RADIUS server.

- **Primary Server Port**

Enter the port number for the primary RADIUS server, or increment/decrement the number using the UP and DOWN arrows.

- **Primary Shared Secret**
Enter the primary shared secret. This is the secret that the external RADIUS server will be using.
- **Verify Primary Secret**
Retype your Primary Secret in this field to verify that you typed it correctly.
- **Secondary RADIUS Server**
(Optional) Repeat the instructions in the previous four bullets to define a Secondary RADIUS Server, if available.
- **Admin RADIUS Timeout**
Enter the maximum idle time (in seconds) before the RADIUS session times out. The default is 600 seconds.
- **Admin RADIUS Authentication Type**
Select the protocol used for authentication of administrators, **CHAP** or **PAP** (the default).
 - PAP (Password Authentication Protocol), is a simple protocol. PAP transmits ASCII passwords over the network “in the clear” (unencrypted) and is therefore considered insecure.
 - CHAP (Challenge-Handshake Authentication Protocol) is a more secure protocol. The login request is sent using a one-way hash function.

Saving Your Security Policy

When you have configured all of your security policy settings, click on the **Apply** button in the Security window to save the new policy.

SSIDs

From the **Configuration>Policies** node in the tree, click on **SSIDs** to display the SSIDs window. This window contains a list of all SSID policies currently available, with tools to manage these policies.

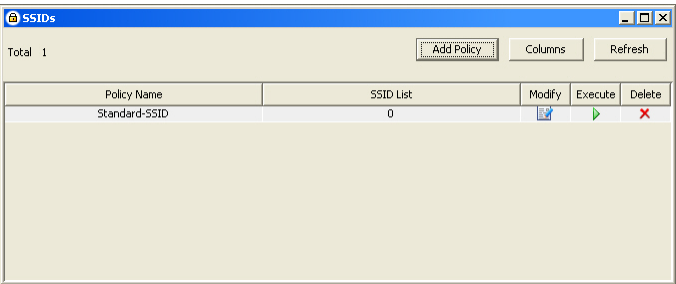


Figure 191. List of SSID Policies

The columns in this window show selected settings for the listed policies. For information about changing the columns displayed, see [“Selecting the Columns Shown in a Policy Window” on page 220](#).

Creating a New SSID Policy

An SSID (Service Set Identifier) is a unique name shared among all devices in a wireless network to establish and maintain wireless connectivity. SSIDs are also known as network names. An SSID policy is created so that you can build a predefined list of SSIDs and manage your SSIDs more conveniently. When an SSID policy is established, all SSIDs contained within the policy are automatically recognized by any Arrays assigned to that policy. To display the SSID Settings window and create a new SSID policy, click on the **Add Policy** button in the SSID Policy window. When the Add Policy window appears, select **Copy from a chosen Array (recommended)** and choose a model Array, or select **Start from scratch**, as described in [“Adding a Policy” on page 219](#). Click **OK**. The policy details window appears.

The creation of different network names (SSIDs) allows system administrators to separate types of users with different requirements. The following characteristics can be tied to an SSID:

- The wireless QoS priority desired for the SSID.
- The wired VLAN associated with the SSID.
- The wireless security mode needed to join the SSID.

We recommend that you define the settings that you will be using before proceeding to create the SSID policy. For example, an SSID may specify a particular VLAN, DHCP pool, filter list, and/or roaming layer. Those should be configured before defining an SSID that will use them.

NOTE:** The SSID policy defines a set of SSIDs. When the policy is applied to an Array, the Array is set to have **exactly** this set of SSIDs. Thus, **any previous SSID configurations on the Array will be deleted, and will be replaced by the SSIDs configured in the policy.

*If you wish to make a change to existing configuration on an Array, rather than replacing that aspect of its configuration, don't use a policy. Instead, see **"Configuring an Array"** on page 174.*

SSID Settings

This window contains a field for defining the name of the policy and an editable table listing all SSIDs currently assigned to this policy.

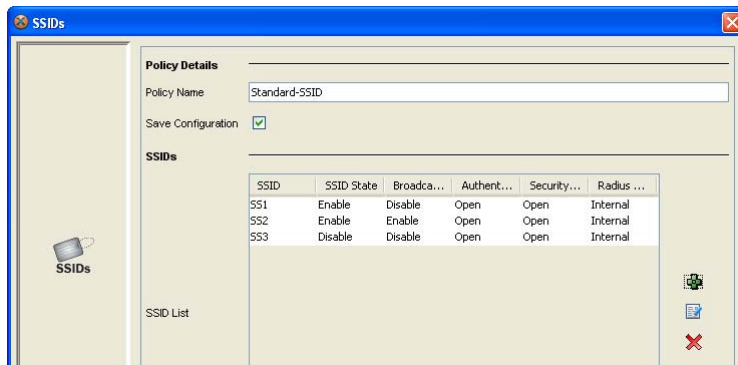


Figure 192. SSID Settings

Policy Details


- **Policy Name**

Enter a meaningful name that describes this policy. If you are modifying an existing policy this field is grayed out (not editable). If you are using a standard naming convention for all of your policies, the name you enter here should conform to that convention.

- **Save Configuration**

Check this box to ensure that any time this policy is applied to an Array, the Array will save the updated configuration information to its flash memory. If this box is left unchecked, then when this policy is applied to Arrays the configuration changes will need to be saved manually or else they will be lost when the Arrays are rebooted. Note that this checkbox does not actually apply the policy to any Arrays. To apply the policy, see [“Using Policy Windows” on page 218](#).

SSID List Details

To add a new SSID, click on the  button to display the SSID List window.

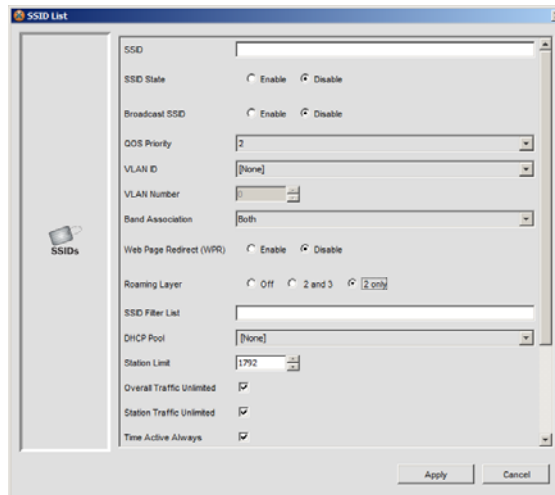


Figure 193. SSID List Entry

- **SSID and SSID State**

Enter a new SSID definition in this field. SSID definitions are case-sensitive and can contain up to 32 alphanumeric characters (do not include spaces when defining SSIDs). Set SSID State to **Enable** to make this SSID active.

- **Broadcast SSID**

Use the **Enable** button if you want to broadcast the SSID. If you do not want other wireless users to see this SSID, leave the box unchecked. The default is not to broadcast the SSID.

- **QoS Priority**

Enter a value in this field for QoS (Quality of Service) priority filtering, or increment/decrement the value using the UP and DOWN arrows. For detailed information on the operation of QoS on the Wi-Fi Array, please see the *Wi-Fi Array User's Guide*, part number 800-0006-001. The QoS value must be one of the following:

- **0**
Low priority 802.1p traffic (user priority 1) is assigned to QoS level 0. Since this background traffic is explicitly designated as low-priority and non-delay sensitive, it is given the lowest traffic class.
- **1**
Best Effort—the default 802.1p user priority (0) is assigned to QoS level 1. For the default priority, we don't necessarily know anything about the type of traffic and it has not been explicitly designated as low-priority traffic. Thus, it is treated as best effort traffic.
- **2**
High, where QoS filtering normally gives priority to video traffic.
- **3**
The highest QoS priority setting, where QoS filtering normally gives priority to voice (VoIP) traffic.

The QoS setting you define here will prioritize wireless traffic for this SSID over other SSID traffic. The default value for this field is 2, which is high (but not highest) priority.

- **VLAN ID / VLAN Number**

If desired, enter a VLAN ID (or select **NUMERIC** and enter a **VLAN Number**) in these fields. Traffic will be forwarded to this VLAN on the wired network. The default value for this field is 0.

- **Band Association**

This option allows you to choose which wireless band the SSID will be beacons on. Make your choice from the pull-down list, either 5 GHz, 2.4 GHz, or Both.

- **Web Page Redirect (WPR)**

Choose **Enable** if you want to use the Web Page Redirect (WPR) functionality. This feature may be used to provide an alternate mode of authentication, or to simply display a splash screen when a user first associates to the wireless network. After that, it can (optionally) redirect the user to an alternate URL. For example, some wireless devices and users may not have a correctly configured 802.1X (RADIUS) supplicant. Utilizing WPR's Web-based login, users may be authenticated without using an 802.1X supplicant. For an in-depth discussion, please see the *Xirrus Web Page Redirect Application Note* in the [Xirrus Library](#).

If you enable WPR, the SSID Management window displays additional fields that must be configured.

If enabled, Web Page Redirect will display a splash or login page when a user associates to the wireless network and opens a web browser to any URL (provided the URL does not point to a resource directly on the user's machine). The user-requested URL is captured, the user's browser is redirected to the splash or login page, and then the browser is redirected either to your specified landing page, if any, or else back to the captured URL. The landing page may be specified for **User Groups** as well. Note that if you change an Array's management HTTPS port, WPR uses that port, too.

You may select among four different modes for use of the Web Page Redirect feature, each displaying a different set of parameters that must be entered:

- **Internal Splash page**

This option displays a splash page instead of the first user-requested URL. The splash page files reside on the Array. Note that XMS has a **Web Page Redirect (WPR)** policy that allows you to replace the default splash page on Arrays, if you wish.

To set up use of a splash page, set **WPR Mode** to **Internal** and set **WPR Screen Type** to **Splash**. Additional fields will be displayed for configuring splash page usage. Enter a value in the **WPR Splash Timeout** field to define how many seconds the splash screen is displayed before timing out, or select **Never** to prevent the page from timing out automatically. After the splash page, the user is redirected to the captured URL. If you want the user redirected to a specific landing page instead, enter its address in **WPR Landing Page URL**.

You may customize this page with a logo and/or background image, and header and/or footer text, as described in [“Customizing an Internal Login or Splash page” on page 299](#).

- **Internal Login**

This option displays a login page (residing on the Array) instead of the first user-requested URL. If you wish to replace the default login page on Arrays, XMS has a **Web Page Redirect (WPR)** policy to upload your custom page.

To set up internal login, set **WPR Mode** to **Internal**, and set **WPR Screen Type** to **Login**. Set **WPR HTTPS Login** to **Enable** for a secure login, or select **Disable** to use HTTP.

Select the **WPR Authentication Protocol**. This is the protocol used for authentication of users, **CHAP** or **PAP** (the default).

- **PAP** (Password Authentication Protocol), is a simple protocol. PAP transmits ASCII passwords over the network

“in the clear” (unencrypted) and is therefore considered insecure.

- **CHAP** (Challenge-Handshake Authentication Protocol) is a more secure Protocol. The login request is sent using a one-way hash function.

The user name and password are obtained by the login page, and authentication occurs according to the **RADIUS Details** in effect for the SSID (see **“RADIUS Details” on page 298**). If Security Settings are set to Global, then the Array’s global RADIUS settings will be used instead (See **“Security Settings” on page 296**).

After authentication, the browser is redirected back to the captured URL. If you want the user redirected to a specific landing page instead, enter its address in **WPR Landing Page**.

You may customize this page with a logo and/or background image, and header and/or footer text, as described in **“Customizing an Internal Login or Splash page” on page 299**.

- **External Login page**

This option redirects the user to a login page on an external web server for authentication, instead of the first user-requested URL. Login information (user name and password) must be obtained by that page, and returned to the Array for authentication.

Authentication occurs according to the **RADIUS Details** currently in effect for the SSID (see **“RADIUS Details” on page 298**). If Security Settings are set to Global, then the Array’s global RADIUS settings will be used instead (See **“Security Settings” on page 296**). After authentication, the browser is redirected back to the captured URL. If you want the user redirected to a specific landing page instead, enter its address in **WPR Landing Page URL**.

To set up external login page usage, set **WPR Mode** to **External**. Set **WPR HTTPS Login** to **Enable** for a secure login, or select **Disable** to use HTTP. Enter the URL of the external web server in **WPR Redirect URL**, enter that server’s shared secret in **WPR Redirect Password**, and enter the **WPR Verify Key**.

Select the **WPR Authentication Protocol**. This is the protocol used for authentication of users, **CHAP** or **PAP** (the default).

- **PAP** (Password Authentication Protocol), is a simple protocol. PAP transmits ASCII passwords over the network “in the clear” (unencrypted) and is therefore considered insecure.
- **CHAP** (Challenge-Handshake Authentication Protocol) is a more secure Protocol. The login request is sent using a one-way hash function.

- **External Splash page**

This option displays a splash page instead of the first user-requested URL. The splash page files reside on an external web server.

To set up external splash page usage, set **WPR Mode** to **External**. Enter the URL of the external web server in **WPR Redirect URL**, enter that server’s shared secret in **WPR Redirect Password**, and enter the **WPR Verify Key**.

After the splash page, the user is redirected to the captured URL. If you want the user redirected to a specific landing page instead, enter its address in **WPR Landing Page URL**.

- **Roaming Layer**

For this SSID, select whether to enable fast roaming between IAPs or Arrays at Layer 2 and Layer 3, or at Layer 2 only. If you select fast roaming at Layers 2 and 3, you must also enable roaming at both layers in RF settings—see “**Global RF Settings**” on page 319. Please see the *Wi-Fi Array User’s Guide* for more information about roaming.

- **SSID Filter List**

To specify filters to be active on this SSID, enter the name of the desired filter list. The filter list should already have been defined before it can be assigned. See “**Filters**” on page 348.

- **DHCP Pool**

If you want to associate an internal DHCP pool to this SSID, choose the pool from the pull-down list. An internal DHCP pool must be created before it can be assigned. See **“DHCP Server” on page 265**.

- **Station Limit**

Enter the maximum number of stations allowed on this SSID. The default is 1792. This step is optional. Note that the IAPs - Global Settings window also has a station limit option—**Max Station Association per IAP**. If both station limits are set, both will be enforced. As soon as either limit is reached, no new stations can associate until some other station has terminated its association.

- **Overall Traffic Unlimited**

Choose **Unlimited** if you do not want to place a restriction on the traffic for this SSID, or enter a value in the **Overall Traffic Packets/Sec Limit** field to force a traffic restriction.

- **Station Traffic Unlimited**

Choose **Unlimited** if you do not want to place a restriction on the traffic per station for this SSID, or enter a value in the **Station Traffic Packets/Sec Limit** field to force a traffic restriction.

- **Time Active**

These options can restrict access to specific days and/or hours.

- **Time Active Always**

Select to allow traffic at any time of day. If this is not selected, then specify the active period using the **Time On** and **Time Off** fields.

- **Active All Days**

Select to allow traffic on all days.

- **Limits by Day**

If **Active All Days** is not selected, then this section is displayed. Choose the days of the week that usage will be permitted.

- **Authentication Type**

The following authentication options are available:

- **Open:** This option provides no authentication and is not recommended.

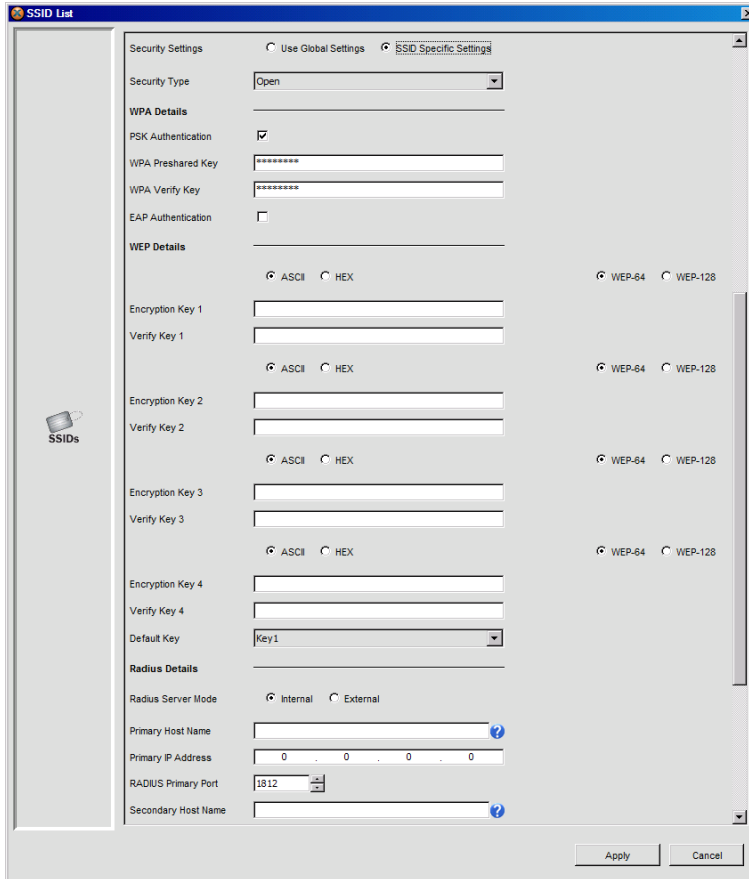
- **RADIUS MAC:** Authenticates stations onto the Wi-Fi network via an external RADIUS server based on the user's MAC address.
- **802.1X:** Authenticates stations onto the Wi-Fi network via a RADIUS server using 802.1X with EAP. The RADIUS server can be internal (provided by the Wi-Fi Array) or external.
- **Security Settings**

You may choose to allow an SSID to use global security settings for its RADIUS server, or override those settings for an SSID. In either case, you may still change the Security Type.

 - **Use Global Settings**

Select this to use the security settings specified for the Array (see [“Configuring an Array” on page 174](#) and [“Security” on page 270](#)).
 - **SSID Specific Settings**

Select this to enter SSID-specific RADIUS server settings that will override the global security settings for this SSID. When you select this option, WPA, WEP, and RADIUS Details sections are displayed, as shown in [Figure 194](#).



SSID List

Security Settings ☐ Use Global Settings ☒ SSID Specific Settings

Security Type: **Open**

WPA Details

PSK Authentication: ☒

WPA Preshared Key:

WPA Verify Key:

EAP Authentication: ☐

WEP Details

☒ ASCII ☐ HEX ☒ WEP-64 ☐ WEP-128

Encryption Key 1:

Verify Key 1:

☒ ASCII ☐ HEX ☒ WEP-64 ☐ WEP-128

Encryption Key 2:

Verify Key 2:

☒ ASCII ☐ HEX ☒ WEP-64 ☐ WEP-128

Encryption Key 3:

Verify Key 3:

☒ ASCII ☐ HEX ☒ WEP-64 ☐ WEP-128

Encryption Key 4:

Verify Key 4:

Default Key: **Key1**

Radius Details

Radius Server Mode: ☒ Internal ☐ External

Primary Host Name:

Primary IP Address:

RADIUS Primary Port:

Secondary Host Name:

Apply **Cancel**

Figure 194. SSID Security Settings

● Security Type

From the pull-down list, choose the level of security that will be required by users of this SSID, and indicate whether the settings apply globally or to the specific SSID. The available options are **Open**, **WEP**, **WPA**, **WPA2**, and **WPA-Both** (where both WPA and WPA2 are used). RADIUS security options are also available. The Open option provides no security and is not recommended. For more information about wireless security, go to **“Security” on page 272**, or see the *Wi-Fi Array User’s Guide*.

- **WPA Details**

This section of the window appears if you have selected **SSID Specific Settings**. Configure WPA encryption as described in “**WPA Details**” on page 273.

- **WEP Details**

This section of the window appears if you have selected **SSID Specific Settings**. Configure WEP encryption as described in “**WEP Details**” on page 274.



*You may specify the RADIUS servers (including accounting servers) by either IP address or host name. To prevent confusion, we recommend that you specify one or the other, but not both. **If you do enter both, only the IP address will be used.** The host name will only be sent to Arrays running ArrayOS Release 3.5 or above.*

- **RADIUS Details**

This section of the window appears if you have selected **SSID Specific Settings**. You may set the RADIUS Server Mode to Internal or External. If you select External, additional fields will be displayed so that you can specify external RADIUS servers. For more information on RADIUS server settings, see “**RADIUS**” on page 276.

- **Accounting**

This section of the window appears if you have selected **SSID Specific Settings** and you set the **RADIUS Server Mode** to **External**. If you click the **On** button for **Accounting**, the Array will send RADIUS Start, Stop, and Interim records to a RADIUS accounting server. Additional fields will be displayed so that you can specify your accounting settings. For more information on accounting settings, see “**External RADIUS Details**” on page 277.

After configuring your SSID parameters, click on the **Apply** button. You are returned to the SSID Settings window where the new SSID is displayed in the list.

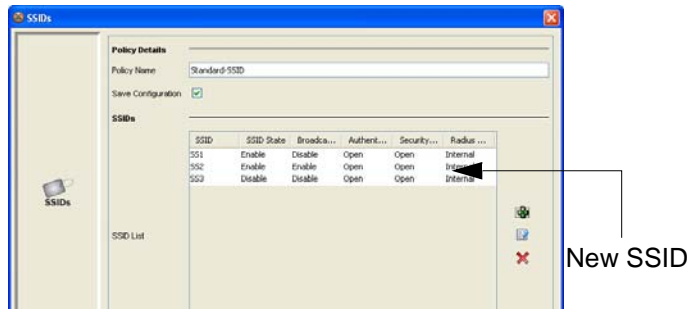


Figure 195. SSID Settings

Customizing an Internal Login or Splash page

You may customize these pages with a logo and/or background image, and header and/or footer text, as shown below in **Figure 196**.

- **WPR Custom Background File**—specify an optional jpg, gif, or png file to display in the background of the page. Other customizations (logo, header, footer) will overlay the background, so that it will not be visible in those areas.
- **WPR Custom Logo File**—specify an optional jpg, gif, or png file to display at the top of the page.
- **WPR Custom Header Text File**—specify an optional .txt file to display at the top of the page (beneath the logo, if any).
- **WPR Custom Footer Text File**—specify an optional .txt file to display at the bottom of the page.

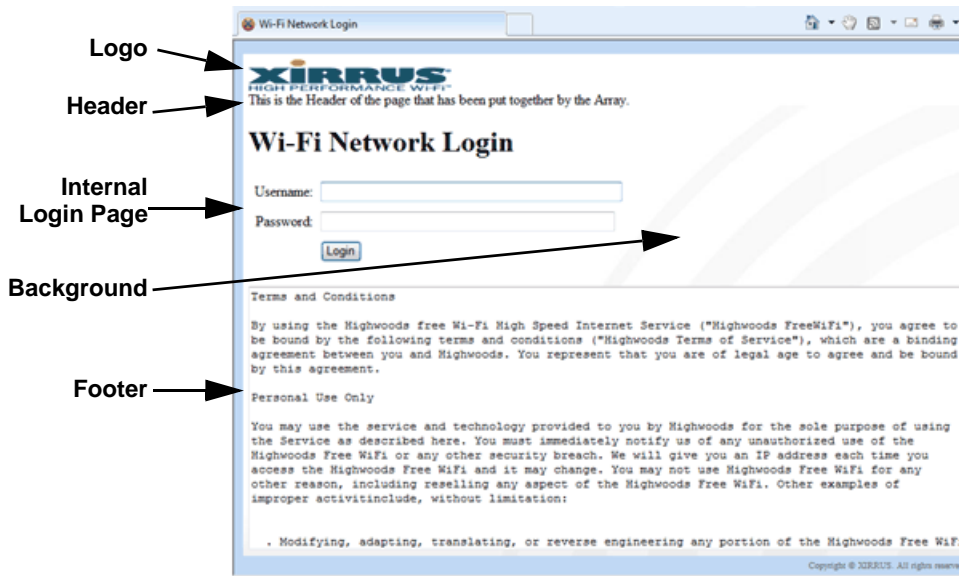


Figure 196. Customizing an Internal Login or Splash Page

Saving Your SSID Policy

When you have configured all of your SSID policy settings, click on the **Apply** button in the SSID window to save the new policy.

User Groups

From the **Configuration>Policies** node in the tree, click on **User Group** to display the User Group window. This window contains a list of all User Group policies currently available, with tools to manage these policies.

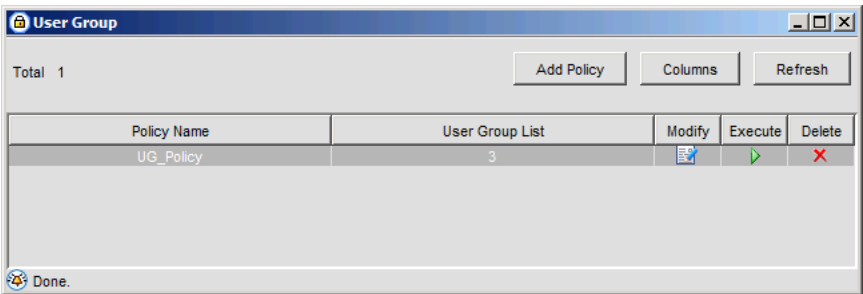


Figure 197. List of User Group Policies

The columns in this window show selected settings for the listed policies. For information about changing the columns displayed, see [“Selecting the Columns Shown in a Policy Window” on page 220](#).

Creating a New User Group Policy

User groups allow administrators to assign specific network parameters to users through RADIUS privileges rather than having to map users to a specific SSID. Groups provide flexible control over user privileges without the need to create large numbers of SSIDs.

A user group also allows you to directly define a uniform set of parameter values to be applied to selected users, rather than via RADIUS accounts. For example, you might define the user group Students, and set its VLAN, security parameters,, and traffic limits. When a new user is created, you can apply all of these settings just by making the user a member of the group.

We recommend that you define the settings that you will be using before proceeding to create the User Group policy. For example, a User Group may specify a particular VLAN, DHCP pool, filter list, and/or roaming layer. Those should be configured before defining a User Group that will use them.

A User Group policy is created so that you can build a predefined list of User Groups and manage User Groups more conveniently. To display the **User Group Settings** window and create a new User Group policy, click the **Add Policy** button in the User Group Policy window. When the Add Policy window appears, select **Copy from a chosen Array (recommended)** and choose a model Array, or select **Start from scratch**, as described in “**Adding a Policy**” on page 219. Click **OK**. The policy details window appears.

***NOTE:** The User Group policy defines a set of User Groups. When the policy is applied to an Array, the Array is set to have **exactly** this set of User Groups. Thus, **any previous User Group configurations on the Array will be deleted**, and will be **replaced** by the User Groups configured in the policy.*

*To change the existing configuration of an Array, rather than replacing that aspect of its configuration, don’t use a policy. Instead, see “**Configuring an Array**” on page 174.*

User Group Settings

This window contains a field for defining the name of the policy and an editable table listing all User Groups currently defined in this policy.

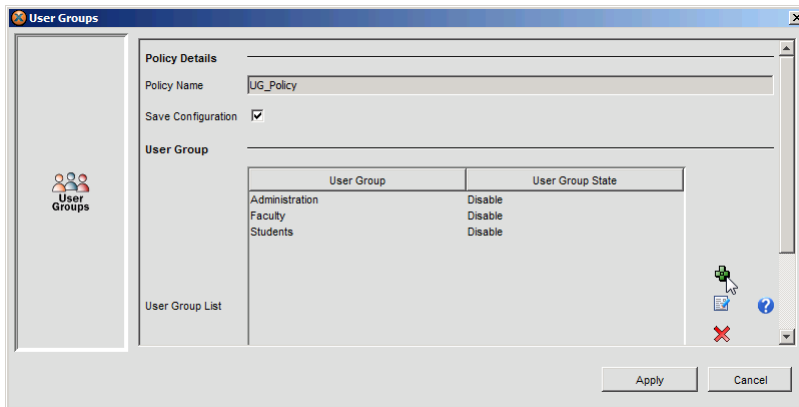


Figure 198. User Group Settings

Policy Details


- **Policy Name**

Enter a meaningful name that describes this policy. If you are modifying an existing policy this field is grayed out (not editable). If you are using a standard naming convention for all of your policies, the name you enter here should conform to that convention.

- **Save Configuration**

Check this box to ensure that any time this policy is applied to an Array, the Array will save the updated configuration information to its flash memory. If this box is left unchecked, then when this policy is applied to Arrays the configuration changes will need to be saved manually or else they will be lost when the Arrays are rebooted. Note that this checkbox does not actually apply the policy to any Arrays. To apply the policy, see [“Using Policy Windows” on page 218](#).

User Group Setting Details

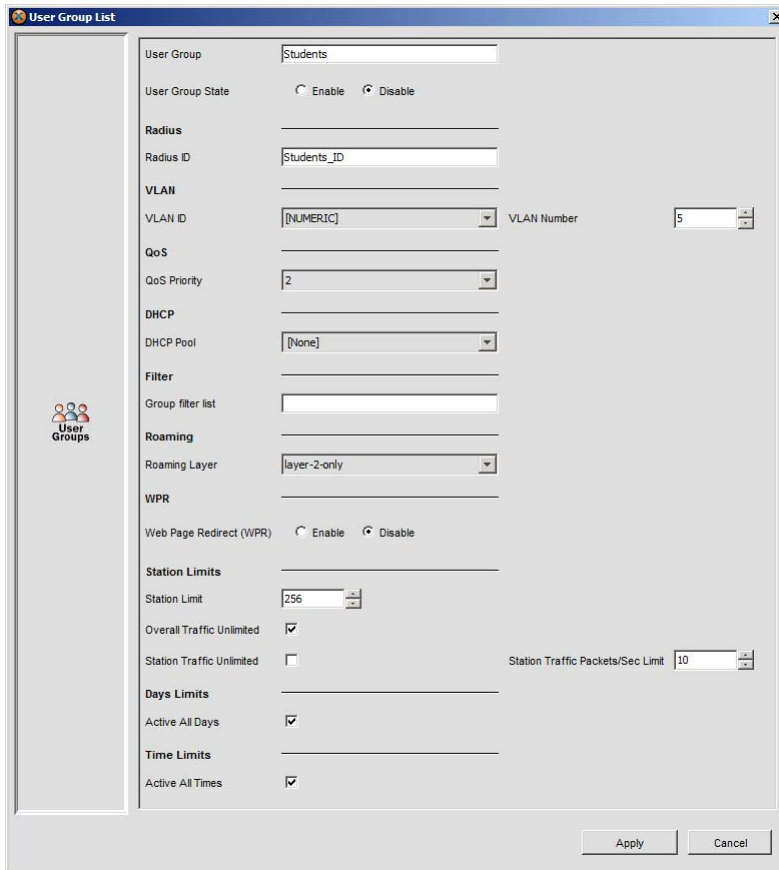
To add a new User Group, click the  button to display the User Group List details window. ([Figure 199](#))

- **User Group and User Group State**

Enter a new User Group name in this field. User Group names are case-sensitive and can contain up to 32 alphanumeric characters (do not include spaces when defining User Groups). Set **User Group State** to **Enable** to make this User Group active.

- **RADIUS ID**

Enter a unique RADIUS ID for the User Group, to be used on an external RADIUS server. When adding a user account to the external RADIUS server, this RADIUS ID value should be entered for the user. When an Array requests authentication of a user, RADIUS sends this value to the Array. This tells the Array that the user is a member of the User Group having this RADIUS ID.



The image shows a 'User Group List' configuration window. On the left is a sidebar with a 'User Groups' icon. The main area contains the following fields and options:

- User Group:** Text field containing 'Students'.
- User Group State:** Radio buttons for 'Enable' and 'Disable'.
- Radius:** Section header.
- Radius ID:** Text field containing 'Students_ID'.
- VLAN:** Section header.
- VLAN ID:** Dropdown menu showing '[NUMERIC]'.
- VLAN Number:** Spin box containing '5'.
- QoS:** Section header.
- QoS Priority:** Dropdown menu showing '2'.
- DHCP:** Section header.
- DHCP Pool:** Dropdown menu showing '[None]'.
- Filter:** Section header.
- Group filter list:** Text field.
- Roaming:** Section header.
- Roaming Layer:** Dropdown menu showing 'layer-2-only'.
- WPR:** Section header.
- Web Page Redirect (WPR):** Radio buttons for 'Enable' and 'Disable'.
- Station Limits:** Section header.
- Station Limit:** Spin box containing '256'.
- Overall Traffic Unlimited:** Checked checkbox.
- Station Traffic Unlimited:** Unchecked checkbox.
- Station Traffic Packets/Sec Limit:** Spin box containing '10'.
- Days Limits:** Section header.
- Active All Days:** Checked checkbox.
- Time Limits:** Section header.
- Active All Times:** Checked checkbox.

At the bottom right are 'Apply' and 'Cancel' buttons.

Figure 199. Adding an entry to the User Group List

- **VLAN ID**

If desired, enter a VLAN ID in this field. Traffic for this User Group will be forwarded to this VLAN on the wired network. The default value for this field is **None**.

- **QoS Priority**

Enter a value in this field for QoS (Quality of Service) priority filtering, or increment/decrement the value using the UP and DOWN arrows. For detailed information on the operation of QoS on the Wi-Fi Array, please

see the *Wi-Fi Array User's Guide*, part number 800-0006-001. The QoS value must be one of the following:

- **0**
The lowest QoS priority setting, where QoS makes its best effort at filtering and prioritizing data, video and voice traffic without compromising the performance of the network. Use this setting in environments where traffic prioritization is not a concern.
- **1**
Medium; QoS prioritization is aggregated across all traffic types.
- **2**
High, where QoS filtering normally gives priority to video traffic.
- **3**
The highest QoS priority setting, where QoS filtering normally gives priority to voice (VoIP) traffic.

The QoS setting you define here will prioritize wireless traffic for this SSID over other SSID traffic. The default value for this field is **2**, which provides high, but not highest, priority.

- **DHCP Pool**

If you want to associate an internal DHCP pool with this User Group, choose the pool from the pull-down list. An internal DHCP pool must be created before it can be assigned. See **"DHCP Server" on page 265**.

- **Filter—Group Filter List**

If you wish to apply filters to this User Group's traffic, enter the name of the desired Filter List. See **"Filters" on page 348**.

- **Roaming**

For this User Group, select whether to enable fast roaming between IAPs or Arrays at Layer 2 and Layer 3, or at Layer 2 only. If you select fast roaming at Layers 2 and 3, you must also enable roaming at both layers in RF settings—see **"Global RF Settings" on page 319**. Please see the *Wi-Fi Array User's Guide* for more information.

- **WPR Enable**

Choose **Enable** if you want this User Group to use the Web Page Redirect (WPR) functionality. This feature may be used to display a splash screen when a user first associates to the wireless network. After that, it can (optionally) redirect the user to an alternate landing page. When you configure WPR for a User Group there is no option to specify a login page, since the user will have been previously authenticated via RADIUS. Except for the lack of login options, the configuration of the WPR feature for a group is similar to its configuration for an SSID. Please see [page 291](#) for more details on WPR. For an in-depth discussion, please see the *Xirrus Web Page Redirect Application Note* in the [Xirrus Library](#).

If you enable WPR, the User Group List window displays additional fields that may be configured.

You may enable or disable use of a splash screen for the Web Page Redirect feature:

- **Enable or disable splash screen for WPR Splash Timeout**

This option displays a splash page instead of the first user-requested URL. The splash page files reside on each Array. Note that XMS has a Web Page Redirect policy that allows you to replace the default splash page on Arrays, if you wish. Please see “[Web Page Redirect \(WPR\)](#)” on [page 358](#) for more information.

To set up use of a splash page, set **Enable or disable splash screen for WPR** to **Enable**. Enter a value in the **WPR Splash Timeout** field to define how many seconds the splash screen is displayed before timing out, or select **0** to prevent the page from timing out automatically. After the splash page, the user is redirected to the captured URL.

- **Landing Page URL for WPR**

If you want the user redirected to a specific landing page rather than to the captured URL (after the splash screen times out, if using a splash screen), enter the landing page address in this field.

Group Limits

The Limits section allows you to limit the traffic or connection times allowed for this User Group. Note that the RF—Global Settings and the SSID policies also have options to limit the number of stations, limit traffic, and/or limit connection times. If limits are set on an Array in more than one place, all limits will be enforced:

- As soon as any station limit is reached, no new stations can associate until some other station has terminated its association.
- As soon as any traffic limit is reached, it is enforced.
- If any connection date/time restriction applies, it is enforced.

You can picture this as a logical AND of all restrictions. For example, suppose that a station's SSID is available MTWTF between 8:00am and 5:00pm, and the User Group is available MWF between 6:00am and 8:00pm, then the station will be allowed on MWF between 8:00am and 5:00pm.

To eliminate confusion, we recommend that you configure limits in just one type of policy.

- **Station Limits**
Enter the maximum number of stations allowed for this User Group. The default is 1792.
- **Overall Traffic Unlimited**
Choose **Unlimited** if you do not want to place a restriction on the traffic for users in this User Group, or clear the checkbox and enter a value in the **Overall Traffic Packets/Sec Limit** field to force a traffic restriction. The restriction applies to the group as a whole. For example, if you limit the Students group to 1000 packets/second, then the sum of the packets sent by all members of the Student group may not exceed 1000 packets/second.
- **Station Traffic Unlimited**
Choose **Unlimited** if you do not want to place a restriction on the traffic per station for this User Group, or clear the checkbox and enter a value in the **Station Traffic Packets/Sec Limit** field to force a traffic restriction.

- **Days/Time Limits**

These options can restrict access to specific days and/or hours.

- **Active All Days**

Select to allow traffic on all days.

- **Limits by Day**

If **Active All Days** is not selected, then this section is displayed. Choose the days of the week that usage will be permitted.

- **Active All Times**

Select to allow traffic at any time of day. If this is not selected, then specify the active period using the **Time On** and **Time Off** fields.

Saving Your User Group Policy

When you have configured all of your User Group policy settings, click on the **Apply** button in the User Group Settings window to save the new policy.

IAPs

All IAPs (Integrated Access Points) within your Arrays are configured with this policy. When you apply an IAP policy, all of the IAPs in the Array will assume the settings defined in the policy, even if you only changed the settings for one IAP when you worked with the policy. Configuration settings for IAPs include enabling or disabling IAPs, defining an IAP’s wireless mode, specifying the channel to be used and the cell size for each, choosing an antenna type, establishing transmit and receive parameters, and providing descriptions.

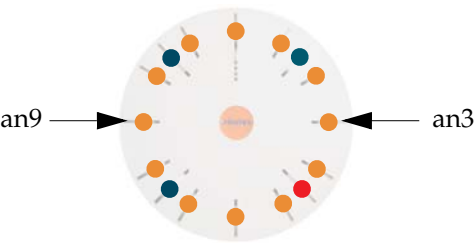


Figure 200. Arrangement of IAPs (XN16 Array)

From the **Configuration>Policies** node in the tree, click on **IAPs** to display the IAPs window. This window contains a list of all IAP policies currently available, with tools to manage these policies.

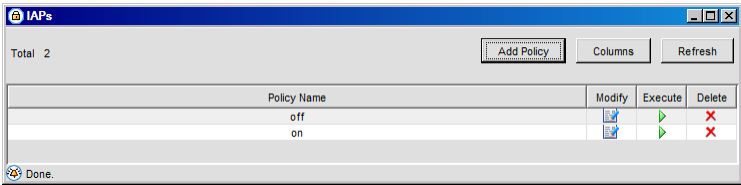


Figure 201. List of IAP Policies

The columns in this window show selected settings for the listed policies. For information about changing the columns displayed, see **“Selecting the Columns Shown in a Policy Window” on page 220**.

Click **Add Policy** on the IAPs window. When the Add Policy window appears, select **Copy from a chosen Array (recommended)** and choose a model Array, or select **Start from scratch**, as described in **“Adding a Policy” on page 219**. Click

OK. The policy details window appears. ((**Figure 202**). This window allows you to select IAPs, one at a time, then establish configuration settings. You may also set all IAPs to be enabled or disabled in one step by using the **Enable All IAPs** or **Disable All IAPs** buttons.

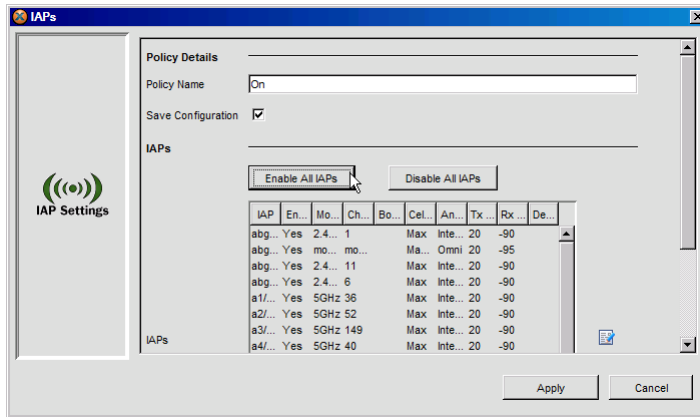


Figure 202. IAP Settings (Policy Details)

In addition to selecting an IAP from the IAP Settings main window, the window provides a convenient at-a-glance snapshot of the attributes associated with each IAP in the list. You can stretch the width of any column to improve the view by simply dragging the column divider in the header row.

To access the IAP Settings pop-up window where configuration settings are established (**Figure 203**), click an IAP to select it and then click the window button to the right of the list (or just double-click an IAP). Make your changes to the IAP, click **Apply**, and then repeat this step for each IAP that you wish to configure. IAPs must be configured in the policy one at a time. You cannot select more than one IAP at a time from the list. Note that even if you have configured settings for all 16 IAPs, settings for inapplicable IAP will be ignored when you apply the policy to an Array. For instance, if you apply the policy to an XN8, then only the settings for **abgn1** to **abgn4** and **an1** to **an4** will be applied to the XN8.

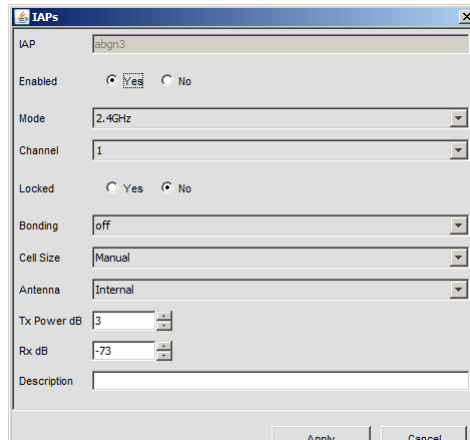


Figure 203. IAP Settings (For Selected IAP)

Policy Details (Figure 202)

- **Policy Name**

Enter a meaningful name that describes this policy. If you are modifying an existing policy this field is grayed out (not editable). If you are using a standard naming convention for all of your policies, the name you enter here should conform to that convention.
- **Save Configuration**

Check this box to ensure that any time this policy is applied to an Array, the Array will save the updated configuration information to its flash memory. If this box is left unchecked, then when this policy is applied to Arrays the configuration changes will need to be saved manually or else they will be lost when the Arrays are rebooted. Note that this checkbox does not actually apply the policy to any Arrays. To apply the policy, see [“Using Policy Windows” on page 218](#).
- **Enable All IAPs / Disable All IAPs**

Use these buttons to enable or disable all IAPs in one step.

IAP Setting Details (Figure 203)

Configure as many IAPs in a policy as you wish, but you must enter the settings for one IAP at a time. Select an IAP from the list in the IAP policy details window.

When you have completed your settings for an IAP, click **Apply**. You may then repeat this to configure as many other IAPs as you wish.

- **IAP**

This field is grayed out (not editable). It identifies the IAP you selected.

- **Enabled**

Choose **Yes** to enable this IAP, or choose **No** to disable this IAP. Disabling IAPs can create coverage patterns to suit the environment. Note that the rest of the fields in this window will be grayed out if the IAP is not enabled.

- **Mode**

Select the wireless mode for this IAP from the choices available in the pull-down menu. The choices are:

- **5GHz**

The IAP will operate at a frequency of 5 GHz with data rates of up to 54 Mbps. This option is available for all IAPs.

- **2.4GHz**

This option is only available for the abg/abgn IAPs. The IAP will operate at a frequency of 2.4 GHz with data rates of up to 54 Mbps. This mode is compatible with the older 802.11b technology, which operates at the same frequency as 802.11g but with a maximum data rate of 11 Mbps. The IAP can also be configured to use just the 802.11g mode, but stations that only support 802.11b will not be able to associate to an IAP configured for 802.11g only.

- **monitor**

The IAP will operate as an RF monitor, scanning for rogue APs in the background. This option is only available on **abg2/abgn2**, where it is the default value. We strongly recommend that you leave **abg2/abgn2** in monitor mode,.

- **Channel**

Because Wi-Fi Arrays are multi-channel devices, allocating the best channels to IAPs is important if peak performance is to be maintained. And to avoid co-channel interference, adjacent IAPs should not be using

adjacent channels—using non-overlapping channels limits interference and delivers maximum capacity.

Select the desired channel for this IAP from the choices available in the pull-down list. If you select the **monitor** option (available on **abg2/abgn2** only—use of the monitor option is strongly recommended!), the IAP will scan all channels for rogue AP devices operating within range of your wireless network.

The channels that are listed for your selection will differ, depending on the country in which Arrays are used. To change the country of operation, select **Admin > Options** from the menu bar. Select the desired **Country** from the drop-down list and click **OK**. A message will be displayed to notify you that you must close your client and start it again. The default country is the United States.

Note that the public safety channels (191 and 195) in the 4.9GHz spectrum range are listed. To use one of these channels, you must first enable the **4.9 GHz Public Safety Band** on the Array, using the RF Global Settings (**“Global RF Setting Details” on page 320**). Operating these channels **requires a license**—using these channels without a license violates FCC rules. Warning notices are displayed when you select these channels.



As mandated by FCC law, Arrays continually scan for signatures of military radar. If such a signature is detected, the Array will switch operation from conflicting channels to new ones.

- **Locked**

Select **Yes** if you want to lock in this channel selection so that the autochannel operation (see **“Global RF Settings” on page 319**) cannot change it.

- **Bonding**

This setting only applies to XN Array models. Also see the discussion of 802.11n bonding in “IEEE 802.11n Deployment Considerations” in the *Xirrus Wi-Fi Array User’s Guide*.

- **Off**—This channel is not bonded to another channel.

- **On**—This channel is bonded to an adjacent channel. The bonded channel is selected automatically by the Array based on current conditions. The choice of banded channel may be dynamic, changing as needed; or it may be static—fixed once the selection is made.
- **+1**—This channel is bonded to the next higher channel number. Auto Channel bonding does not apply.
- **-1**—This channel is bonded to the next lower channel number. Auto Channel bonding does not apply.

- **Cell Size**

The number of users and their applications are major drivers of bandwidth requirements; therefore, you must account for the number of users within an Array's cell diameter when calculating cell sizes.

Select the desired cell size for this IAP from the choices available in the pull-down list, either **Manual**, **Small**, **Medium**, **Large**, or **Max**. Note that the Max option may not be used at the same time as sharp cells (see [“Global RF Setting Details” on page 320](#)).

As a rule, small cell sizes achieve higher data rates. If you choose to define the cell size manually, you must specify the transmit power and receive power in the **Tx Power dB** (transmit) and **Rx dB** (receive) fields.

- **Antenna**

Select an antenna type from the pull-down list, either **Internal**, **External** or **Omni**. The antenna type for the monitoring IAP (**abg2/abgn2**) must be set to Omni. The default for all other IAPs is Internal. Only select the External option if an external antenna is available.

- **Tx Power dB**

The cell size of an IAP is a function of its transmit power and determines the IAP's overall coverage. Adjusting the transmit power allows you to fine tune cell sizes. If many Arrays are in close proximity to each other reduce the transmit power to avoid excessive interference.

Enter a value in this field to define the transmit power (in dB), or increment/decrement the value using the UP and DOWN arrows. The default transmit power is 20 dB.

- **Rx dB**
Enter a value in this field to define the receive power (in dB), or increment/decrement the value using the UP and DOWN arrows. The default receive power is -90 dB.
- **Description** (optional)
If desired, enter a description for this IAP. The IAP assignment (for example, an1, a2, etc.) is not affected by any optional description you enter in this field.

Saving Your IAP Policy

When you have configured all of your IAP policy settings, click on the **Apply** button in the IAP policy details window to save the new policy.

RF

From the **Configuration>Policies** node in the tree, click on **RF** to display the RF window. This window contains a list of all RF policies currently available, with tools to manage these policies.

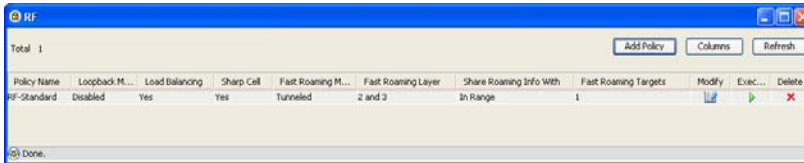


Figure 204. List of RF Policies

The columns in this window show selected settings for the listed policies. For information about changing the columns displayed, see [“Selecting the Columns Shown in a Policy Window” on page 220](#).

How you set up an RF policy will determine how the Arrays assigned with that policy operate within your wireless network, including the coverage patterns generated by the Arrays, the channels they use, and the transmit power. The following graphic shows examples of full and partial coverage patterns.

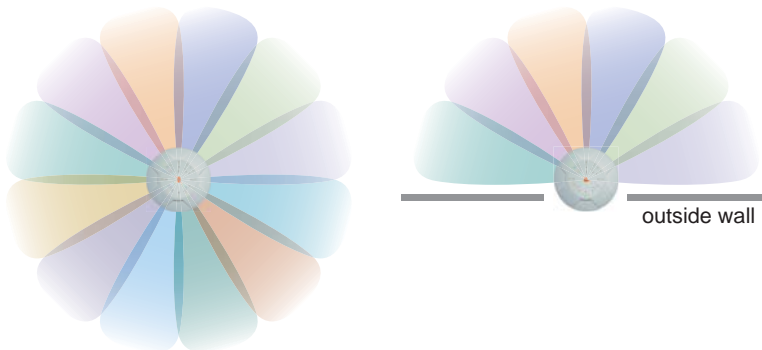


Figure 205. Radiated Coverage Patterns

With a full coverage pattern (left image), all IAPs are activated with coverage spanning 360 degrees. Any client within range will always receive coverage regardless of their geographic position relative to the Array. Partial coverage can be achieved by turning off any combination of IAPs.

Creating a New RF Policy

An RF policy is created so that you can define how your Arrays and the IAPs within the Arrays operate in your wireless network to achieve optimum RF operability in all RF bands. To create a new RF policy, click on the **Add Policy** button in the RF Policy window. When the Add Policy window appears, select **Copy from a chosen Array (recommended)** and choose a model Array, or select **Start from scratch**, as described in [“Adding a Policy” on page 219](#). Click **OK**. The RF policy details window is displayed, and is divided into five primary areas:

- **Global RF Settings**

Configuration settings established here affect the wireless operation of all Arrays to which this policy is applied. Global settings are not specific to an 802.11 wireless technology. Instead, they affect the RF characteristics of Arrays in ways that are common to your wireless network’s operation. This area of the policy defines the name of the policy. It also allows you to change basic RF settings; enable or disable features such as loopback mode (radio assurance), load balancing, sharp cells, station-to-station blocking, and WLAN management; and configure fast roaming parameters.

- **802.11a Settings**

These settings include defining the basic 802.11a data rates, which 802.11a data rates are supported, and specifying the threshold parameters for fragmentation and RTS. Any configuration parameters you establish here will affect all 802.11a IAPs on Arrays to which this policy is assigned.

- **802.11b/g Settings**

These settings include choosing the 802.11g only mode of operation, defining the basic 802.11b and 802.11g data rates and which 802.11b/g data rates are supported, specifying the threshold parameters for fragmentation and RTS, and establishing an 802.11b preamble. Any configuration parameters you establish here will affect all 802.11b and 802.11g IAPs on Arrays to which this policy is assigned.

- **802.11n Settings**

These settings include enabling or disabling 802.11n mode for the entire Array, specifying the number of transmit and receive chains (data stream)

used for spatial multiplexing, setting a short or standard guard interval, auto-configuring channel bonding, specifying whether auto-configured channel bonding will be static or dynamic, and defining the basic 802.11n data rates and which 802.11n data rates are supported. Any configuration parameters you establish here will affect all 802.11n IAPs on Arrays to which this policy is assigned.

● LED Settings

These settings allow you to disable LED activity, define which event triggers the LEDs (either when an IAP is enabled or when a station first associates with the network), and set up the behavior pattern of the LEDs on your Arrays. Any configuration parameters you establish here will affect the LED behavior on all Arrays to which this policy is assigned. The following graphic shows the location of LEDs on an XN16 Wi-Fi Array, which has a total of 16 IAPs.

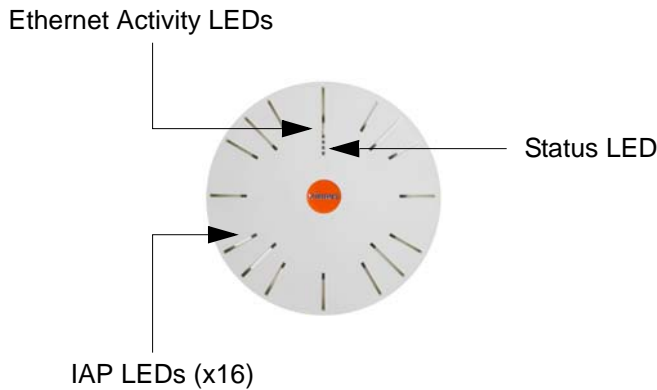


Figure 206. LED Locations (XN16)

Global RF Settings

Global RF settings refer to 802.11a, 802.11b and 802.11g wireless settings that are applied to all IAPs on an Array. This window contains a field for defining the name of the policy and fields for configuring global RF settings.

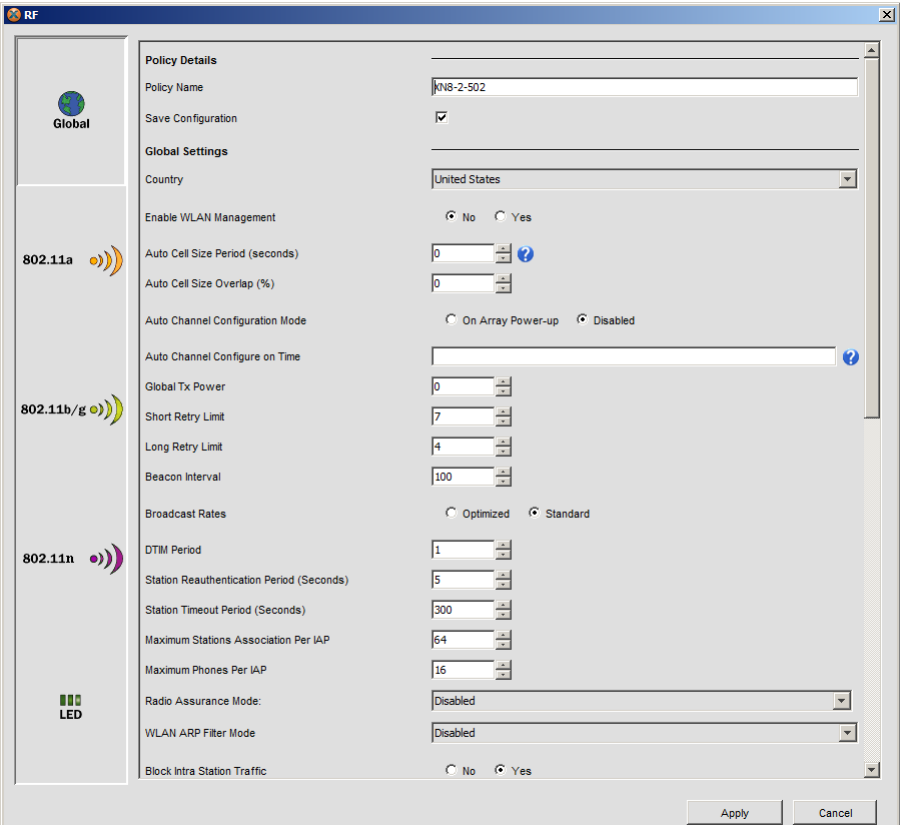


Figure 207. Global RF Settings

Policy Details

● Policy Name

Enter a meaningful name that describes this policy. If you are modifying an existing policy this field is grayed out (not editable). If you are using a standard naming convention for all of your policies, the name you enter here should conform to that convention.

- **Save Configuration**

Check this box to ensure that any time this policy is applied to an Array, the Array will save the updated configuration information to its flash memory. If this box is left unchecked, then when this policy is applied to Arrays the configuration changes will need to be saved manually or else they will be lost when the Arrays are rebooted. Note that this checkbox does not actually apply the policy to any Arrays. To apply the policy, see [“Using Policy Windows” on page 218](#).

Global RF Setting Details

- **Country**

You may choose an Array’s country of operation from the pull-down list. Once a country has been set on an Array, it may not be changed. Please contact Xirrus Customer Support if you need to change the operating country after it has already been set.

The channels that are available for assignment to an IAP will differ, depending on the country of operation. If you set **Country** to **United States**, then 24 channels are available to 802.11a(n) radios. Until you have chosen a country, the Array defaults to channels and power levels that are legal worldwide—this set only includes the lower eight 5 GHz channels.

The country chosen here does not need to be the same as the country selected in [“Country of Operation” on page 496](#). For example, you might run the XMS server in Paris, but set Country in the Global RF Settings to United Kingdom for Arrays operated in London.

- **Enable WLAN Management**

This option allows you to enable or disable WLAN management. If this feature is enabled, any Array with this policy assigned to it can be remotely managed by a client. Choose **Yes** to allow remote management of Arrays, or choose **No** to deny management. The default is **No**.

- **Auto Cell Size Period (seconds)**

You may set up auto cell size configuration to run periodically, readjusting optimal cell sizes for the current conditions. Enter a number

of seconds to specify how often auto-configuration will run. If you select **0**, then auto-configuration of cell sizing will not be run automatically.

- **Auto Cell Size Overlap (%)**

Enter the percentage of cell overlap that will be allowed when the Array is determining automatic cell sizes.

- **Auto Channel Configuration Mode**

This option allows you to instruct the Array to auto-configure channel selection for each enabled IAP when the Array is powered up. Choose **On Array PowerUp** to enable this feature, or choose **Disabled** to disable this feature. See [“Auto-Configuring Channels on Multiple Arrays” on page 181](#) for a discussion of auto configuring channel selection.

- **Auto Channel Configure on Time**

This option allows you to instruct the Array to auto-configure channel selection for each enabled IAP at a time you specify here (in hours and minutes, using the format: hh:mm). Leave this field blank unless you want to specify a time at which the auto-configuration utility is initiated.

- **Global Tx Power**

Enter the transmit power to be used for all IAPs.

- **Short Retry Limit**

This attribute indicates the maximum number of transmission attempts for a frame, the length of which is less than or equal to the RTS Threshold, before a failure condition is indicated. The default value is 7. Enter a new value between 1 and 128, or increment/decrement the value using the UP and DOWN arrows.

- **Long Retry Limit**

This attribute indicates the maximum number of transmission attempts for a frame, the length of which is greater than the RTS Threshold, before a failure condition is indicated. The default value is 4. Enter a new value between 1 and 128, or increment/decrement the value using the UP and DOWN arrows.

- **Beacon Interval**

When an Array sends a beacon it includes with it a beacon interval, which specifies the period of time before it will send the beacon again. The

default value is 100. Enter a new value between 20 and 1000, or increment/decrement the value using the UP and DOWN arrows. The value you enter here is applied to all IAPs.

- **Broadcast Rates**

This option changes the rates of broadcast traffic sent by the Array (including beacons). When set to **Optimized**, each IAP broadcasts at the lowest Array TX data rate currently in use by associated stations, thus improving system performance. For example, if ten stations are associated at 54 Mbps and one station at 12 Mbps, broadcasts will go out at 12Mbps. One out of eight beacons are sent out at the lowest basic rate (1 Mbps for 802.11b/g radios, 6Mbps for 802.11a radios).

When set to **Standard** (the default), broadcasts are sent out at the lowest basic rate only. The option you select here is applied to all IAPs.

- **DTIM Period**

The DTIM (Delivery Traffic Indication Message) is a signal sent as part of a beacon by an Array to a client device in sleep mode, alerting the device to a packet awaiting delivery. The **DTIM Period** is a multiple of the **Beacon Interval**, and it determines how often DTIMs are sent out. By default, the DTIM period is 1, which means that it is the same as the beacon interval. Enter the desired multiple, between 1 and 255. The value you enter here is applied to all IAPs.

- **Station Reauthentication Period (seconds)**

The value in this field specifies a time (in seconds) for the duration of station reauthentications. The default is 5 seconds. Enter a new value (the minimum is 1 second), or increment/decrement the value using the UP and DOWN arrows.

- **Station Timeout Period (seconds)**

The value in this field specifies the elapsed time (in seconds) before the association of an inactive station times out. The default is 300 seconds. Enter a new value (the minimum is 1 second), or increment/decrement the value using the UP and DOWN arrows.

- **Maximum Station Associations Per IAP**

The value in this field defines the maximum number of stations that can associate with each IAP. The default is 96 (maximum), but you can decrease this number if you want to reduce the allowable number of stations per IAP. Reducing this number can improve the performance of your Arrays during times of peak traffic because the value you enter here is applied to all IAPs.



This admission control feature applies only to Spectralink phones. It does not apply to all VoIP phones in general.

- **Maximum Phones Per IAP**

The value in this field defines the maximum number of voice stations that can associate with each IAP. The default is 16 (maximum), but you can decrease this number if you want to reduce the allowable number of phones per IAP. Reducing this number can improve the performance of your Arrays during times of peak traffic because the value you enter here is applied to all IAPs. Note that the maximum number of phones allowed per IAP is lower than the number of other types of stations allowed. This is because VoIP is a real-time application that is very delay-sensitive and highly dependent on the quality of the service it receives. Data loss results in deteriorating voice quality.

- **Radio Assurance Mode**

When Intrusion Detection is set to Standard on an Array (configured on this window, below), self-monitoring is performed (if Radio Assurance Mode is not disabled). IAP **abg2/abgn2** performs loopback tests on the Array's other radios. Tests include sending a probe to another radio and checking for a response, and verifying that beacons are received from the other radio. For more information, please see Array Monitor and Loopback Testing Capabilities in Appendix C of the *Wi-Fi Array User's Guide*.

The loopback mode scans and sends out probe requests on each channel, in turn. It listens for all probe responses and beacons. These tests are performed continuously (24/7). If no beacons or probe responses are

observed from a radio for a predetermined period, loopback mode will take action according to the preference that you have specified.

The following loopback mode options may be configured:

- **Disabled**—Disable IAP loopback tests (no self-monitoring occurs). Loopback tests are disabled by default.
 - **Failure alerts only**—The Array will issue alerts in the Syslog, but will not initiate repairs or reboots.
 - **Failure alerts & repairs, but no reboots**—The Array will issue alerts and perform resets of one or all of the radios if needed.
 - **Failure alerts & repairs & reboots if needed**—The Array will issue alerts, perform resets, and schedule reboots if needed.
- **WLAN ARP Filter Mode**

Address Resolution Protocol finds the MAC address of a device with a given IP address by sending out a broadcast message requesting this information. ARP filtering on an Array allows you to reduce the proliferation of ARP messages by restricting how they are forwarded across the network.

You may select the following options for handling ARP requests on Arrays:

- **Disabled:** ARP filtering is disabled. ARP requests are broadcast to stations. This is the default value.
- **Pass-through:** The Array forwards the ARP request. It passes along only ARP messages that target the stations that are associated to it.
- **Proxy:** The Array replies on behalf of the stations that are associated to it. The ARP request is not broadcast to the stations.

Note that the Array has a broadcast optimization feature that is always on (it is not configurable). Broadcast optimization restricts all broadcast packets (not just ARP broadcasts) to only those radios that need to forward them. For instance, if a broadcast comes in from VLAN 10, and there are no VLAN 10 users on a radio, then that radio will not send out that broadcast. This increases available air time for other traffic.

- **Block Intra Station Traffic**

This option allows you to block or allow traffic between wireless clients that are associated to any Array using this policy. Choose **Yes** to block traffic between stations. Internet access and other access beyond the Array is allowed, but access is blocked between stations associated to IAPs on the same Array. Choose **No** to allow traffic between stations. The default is No.

- **Load Balancing**

The Xirrus Wi-Fi Array supports an automatic load balancing feature designed to distribute Wi-Fi stations across multiple radios rather than having stations associate to the closest radios with the strongest signal strength, as they normally would. In Wi-Fi networks, the station decides to which radio it will associate. The Array cannot actually force load balancing, however the Array can “encourage” stations to associate in a more uniform fashion across all of the radios of the Array. This option enables or disables active load balancing between the Array IAPs. For an in-depth discussion, see the *Xirrus Station Load Balancing Application Note* in the [Xirrus Library](#).

Choose **Passive** to enable standard load balancing. If the Array decides that an IAP is overloaded, that IAP will not respond immediately to a client’s Probe request. After a few seconds, if the client has still not associated the IAP will respond, assuming that this client is determined to associate to the overloaded IAP. Overloaded IAPs will always respond to Association and Authentication requests.

If you select **Active** Load Balancing and an IAP is overloaded, that IAP will send an “AP Full” message in response to Probe, Association, or Authentication requests. This mode is useful because it prevents determined clients from forcing their way onto overloaded IAPs. Note that some clients are so determined to associate to a particular IAP that they will not try to associate to another IAP, and thus they never get on the network.

Choose **Off** to disable load balancing.

- **Sharp Cell**

This option allows you to enable or disable the use of sharp cells. If this feature is enabled, the RF signal for each data rate is tuned to end at a defined boundary (cell size). This reduces interference between nearby cells that use the same channel on other Arrays or other neighboring access points. Sharp cell technology suppresses interference from longer “slower” data rates and improves data-rate performance for end users by enforcing high data-rate cells. It does decrease range of the cell, however.

Choose **Yes** to enable sharp cells. The default is Yes - sharp cell usage is recommended in most cases. Note that Cell Size may **not** be set to Max if Sharp Cell is enabled. See [“IAP Setting Details \(Figure 203\)” on page 311](#).

- **802.11h Beacon Support**

This option enables beacons on all of the Array’s radios to conform to 802.11h requirements, supporting dynamic frequency selection (DFS) and transmit power control (TPC) to satisfy regulatory requirements for operation in Europe.

- **4.9 GHz Public Safety Band**

This option adds two new channels (191 and 195) in the 4.9GHz spectrum range for public safety usage by qualified organizations. Operating these channels **requires a license**, and so they are not for general purpose use. Using these channels without a license violates FCC rules. Warning notices are displayed when you enable this feature and select these channels. All 802.11an and 802.11a/b/g/n radios may be set to these channels.

- **Intrusion Detection**

This option allows you to set the intrusion detection method used on an Array, either **Standard** or **Disable**.

- **Standard**—enables the **abg2/abgn2** radio as a monitor which collects Rogue AP information.

In addition, Standard mode enables self-monitoring. The Array uses the built in monitor radio (IAP **abg2/abgn2**) to periodically associate to other radios in the Array to verify proper operation. In this mode if

a problem is detected, corrective actions are taken to recover—if any radio is found to be operating improperly, the Array will reset it and issue an alert in the Syslog. For more details, see “Configuring Self-Monitoring Mode (Loopback Tests)” in Chapter 5 of the *Xirrus Wi-Fi Array User’s Guide*.

- **Disable**—IAP **abg2/abgn2** does not function as a monitor.
- **Auto Block Unknown Rogue APs**
This setting will only be displayed if you have set **Intrusion Detection** to **Standard**.

An Array can block a rogue AP by taking measures to prevent stations from staying associated to the rogue. When the monitor radio **abg2/abgn2** is scanning, any time it hears a beacon from a blocked rogue **abg2/abgn2** sends out a broadcast “death” signal using the rogue’s BSSID and source address. This has the effect of disconnecting all of a rogue AP’s clients approximately every 5 to 10 seconds, which is enough to make the rogue frustratingly unusable.

When the Auto Blocking option is enabled on an Array, it treats unknown APs as if they were explicitly blocked. This is basically a “shoot first and ask questions later” mode. By default, auto blocking is turned off. Auto blocking provides two parameters for qualifying blocking so that APs must meet certain criteria before being blocked. This keeps the Array from blocking every AP that it detects.

- **Auto Block RSSI**—Sets a minimum RSSI value for automatic blocking of rogue APs. For example, if an AP has an RSSI value of -90, it is probably a harmless AP belonging to a neighbor and not in your building. The default value is -50.
- **Auto Block Level**—Block based on encryption level. Select an encryption level from the drop-down list—rogues meeting this criterion will be blocked.
- **Auto Block Network Types**—Select rogue APs to automatically block by applying the criteria above only to networks of the type specified below. The choices are:

- **All**—the unknown rogue APs may be part of any wireless network.
- **IBSS/AD Hoc only**—only consider auto blocking rogue APs if they belong to an ad hoc wireless network (a network of client devices without a controlling Access Point, also called an Independent Basic Service Set—IBSS).
- **ESS/Infrastructure only**—only consider auto blocking rogue APs if they are in infrastructure mode rather than ad hoc mode.
- **Fast Roaming Mode**

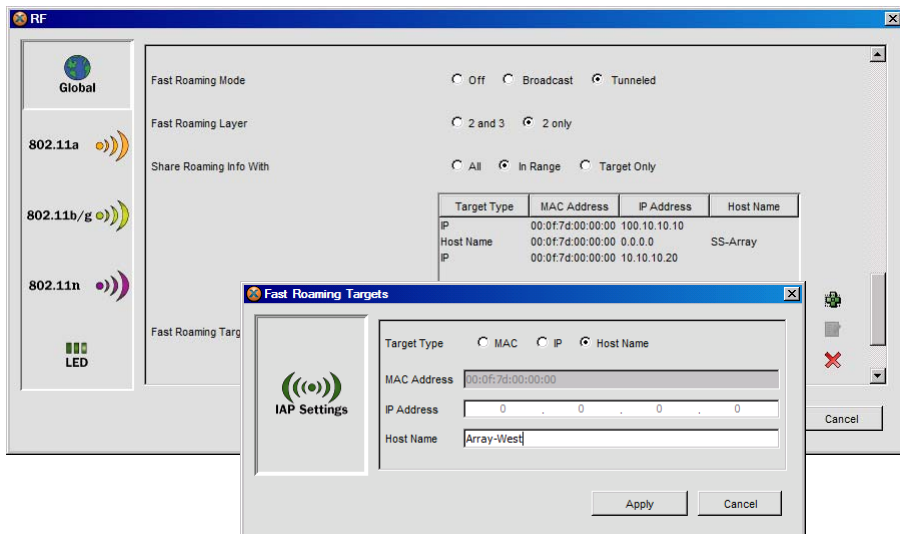


Figure 208. Fast Roaming Settings

This feature utilizes the Xirrus Roaming Protocol (XRP) ensuring fast and seamless roaming capabilities between IAPs or Arrays at Layer 2 and Layer 3, while maintaining security. Fast roaming eliminates long delays for re-authentication, thus supporting time-sensitive applications such as Voice over Wi-Fi (see “Understanding Fast Roaming” in the *Wi-Fi Array User’s Guide* for a discussion of this feature). XRP uses a discovery process to identify other Xirrus Arrays as fast roaming targets. This feature has three modes:

- **Broadcast**—the Array uses a broadcast technique to discover other Arrays that may be targets for fast roaming.
- **Tunneled**—in this Layer 3 technique, fast roaming target Arrays must be explicitly specified.
- **Off**—this disables fast roaming.

To enable fast roaming, set **Fast Roaming Mode** to **Broadcast** or **Tunneled**, and set additional fast roaming attributes below.

If you enable fast roaming, the following ports **cannot** be blocked by firewalls:

- **Port 22610**—reserved for Layer 2 roaming using UDP to share PMK information between Arrays.
- **Ports 15000 to 17999**—reserved for tunneling between subnets.


- **Fast Roaming Layer**

If fast roaming is in Tunneled mode, select whether to enable roaming capabilities between IAPs or Arrays at Layer 2 and Layer 3, or at Layer 2 only. Depending on your wired network, you may wish to allow fast roaming at Layer 3. This may result in delayed traffic. The default is **2 only**.

- **Share Roaming Info With**

If Fast Roaming is in Tunneled mode, this option allows an Array to share roaming information with all Arrays, just Arrays that are within range, or specifically targeted Arrays. Choose either **All**, **In Range** (this is the default) or **Target Only**, as desired.

- **Fast Roaming Targets**

If you chose **Target Only**, use this option to add target Arrays. Click the  button to add each target Array, then click **Apply** after each addition. Add as many targets as you like.

A target Array may be specified using the Array's **MAC Address**, **IP Address**, or **Host Name**. Use the radio buttons to select a format, and then enter the address in the appropriate form. (Figure 208)

To delete a target, select it from the list, then click the **X** icon.

After completing all of the desired fields in the Global window, either click on the **Apply** button to save this policy or click on one of the following buttons to configure more RF policy options:

- **802.11a Settings**
Configure settings for the 802.11a wireless technology.
- **802.11b/g Settings**
Configure settings for the 802.11b and 802.11g wireless technologies.
- **802.11n Settings**
Configure settings for the 802.11n wireless technology.
- **LED Settings**
Configure the activity parameters and behavior of Array LEDs.

802.11a Settings

This window allows you to establish global 802.11a IAP settings. These settings include defining the basic 802.11a data rates, which 802.11a data rates are supported, and specifying the threshold parameters for fragmentation and RTS. Any configuration parameters you establish here will affect all 802.11a IAPs on the Array when this policy is assigned.

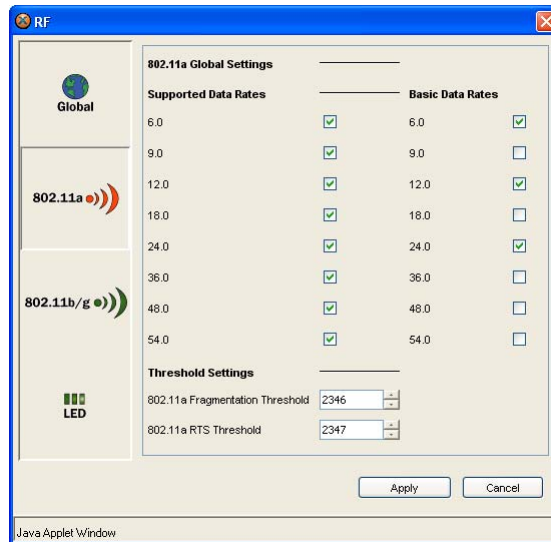


Figure 209. 802.11a RF Settings

802.11a Global Setting Details

- **Supported Data Rates**

The data rates that are enabled here are the 802.11a data rates that your Arrays will use for transmissions to clients on the network. Check or uncheck the boxes to define which data rates are supported. The default is for all 802.11a data rates to be supported.

- **Basic Data Rates**

The data rates that are enabled here define the minimum set of 802.11a data rates that a wireless station must support if it wants to associate with the Arrays. Check or uncheck the boxes to define the basic data rates

required by an 802.11a client. The default for the basic 802.11a data rates is to have 6 Mbps, 12 Mbps and 24 Mbps enabled.

802.11a Threshold Setting Details

- **802.11a Fragmentation Threshold**

This is the maximum size for directed data packets transmitted over 802.11a IAPs. Larger frames fragment into several packets, with their maximum size defined by the value you enter here. Smaller fragmentation numbers can help to “squeeze” packets through in noisy environments.

Enter a value in this field, between 256 and 2346, or increment/decrement the value using the UP and DOWN arrows. The value you enter here will define the fragmentation threshold for all 802.11a IAPs. The default is 2346.

- **802.11a RTS Threshold**

The RTS (Request To Send) threshold specifies the packet size. Packets larger than the RTS threshold will use CTS/RTS prior to transmitting the packet—useful for larger packets to help ensure the success of their transmission.

Enter a value in this field, between 1 and 2347, or increment/decrement the value using the UP and DOWN arrows. The value you enter here will define the RTS threshold for all 802.11a IAPs. The default is 2347.

After completing all of the desired fields in the 802.11a Settings window, either click on the **Apply** button to save this policy or click on one of the following buttons to configure more RF policy options:

- **802.11b/g Settings**

Configure settings for the 802.11b and 802.11g wireless technologies.

- **802.11n Settings**

Configure settings for the 802.11n wireless technology.

- **LED Settings**

Configure the activity parameters and behavior of Array LEDs.

802.11b/g Settings

This window allows you to choose the 802.11g only mode of operation, define the basic 802.11b and 802.11g data rates and which 802.11b/g data rates are supported, specify the threshold parameters for fragmentation and RTS, and establish an 802.11b preamble. Any configuration parameters you establish here will affect all 802.11b and 802.11g IAPs in the Array when this policy is assigned.

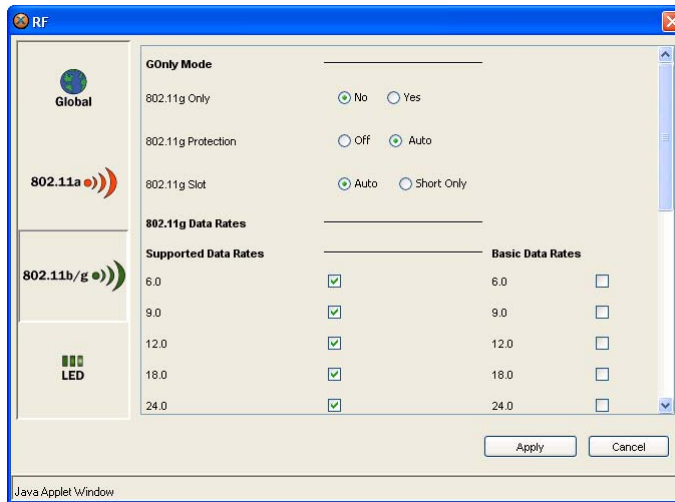


Figure 210. 802.11 /g RF Settings

G Only Mode

- **802.11g Only**

Choose **Yes** if you want to restrict the use of 802.11b/g IAPs to the 802.11g mode only. In this mode, no 802.11b rates are transmitted, and stations that only support the 802.11b wireless technology will not be able to associate to the Arrays. Choose **No** if you want to allow inter-operability with 802.11b clients. The default for this option is No.

- **802.11g Protection**

This is a mechanism to let 802.11g IAPs know when they should use modulation techniques to communicate with 802.11b devices, especially

in wireless networks where there is a mixed environment that has 802.11g and 802.11b clients (and the clients are hidden from each other).

Choose **Auto** to enable automatic protection for all 802.11g IAPs. If you disable the 802.11g protection feature, this assumes there are no wireless stations using the 802.11b technology. When operating in a mixed 802.11b/g environment with minimal 802.11b traffic, choose **Off** to ensure the best performance for your 802.11g stations.

- **802.11g Slot**

802.11g wireless technology defines a long slot time as 20 microseconds and a short slot time as 9 microseconds. 802.11b wireless technology only supports the long slot time of 20 microseconds.

In mixed 802.11b and 802.11g environments, choose **Auto** to instruct the Arrays to manage the 802.11g slot time automatically. In an 802.11g only environment, choose the **Short Only** option for better performance, giving precedence to 802.11g traffic. The default is Auto.

802.11g Data Rates

- **Supported Data Rates**

The data rates that are enabled here are the 802.11g data rates that your Arrays will use for transmissions to clients on the network. Check or uncheck the boxes to define which data rates are supported. The default is for all 802.11g data rates to be supported.

- **Basic Data Rates**

The data rates that are enabled here define the minimum set of 802.11g data rates that a wireless station must support if it wants to associate with the Arrays. Check or uncheck the boxes to define the basic data rates required by an 802.11g client. The default is to have all basic 802.11g data rates disabled.

802.11b Data Rates

- **Supported Data Rates**

The data rates that are enabled here are the 802.11b data rates that your Arrays will use for transmissions to clients on the network. Check or

uncheck the boxes to define which data rates are supported. The default is for all 802.11b data rates to be supported.

- **Basic Data Rates**

The data rates that are enabled here define the minimum set of 802.11b data rates that a wireless station must support if it wants to associate with the Arrays. Check or uncheck the boxes to define the basic data rates required by an 802.11b client. The default is to have all basic 802.11b data rates enabled (1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps).

802.11b/g Threshold Setting Details

- **802.11bg Fragmentation Threshold**

This is the maximum size for directed data packets transmitted over 802.11b/g IAPs. Larger frames fragment into several packets, with their maximum size defined by the value you enter here. Smaller fragmentation numbers can help to “squeeze” packets through in noisy environments.

Enter a value in this field, between 256 and 2346, or increment/decrement the value using the UP and DOWN arrows. The value you enter here will define the fragmentation threshold for all 802.11b/g IAPs. The default is 2346.

- **802.11bg RTS Threshold**

The RTS (Request To Send) threshold specifies the packet size. Packets larger than the RTS threshold will use CTS/RTS prior to transmitting the packet—useful for larger packets to help ensure the success of their transmission.

Enter a value in this field, between 1 and 2347, or increment/decrement the value using the UP and DOWN arrows. The value you enter here will define the RTS threshold for all 802.11a IAPs. The default is 2347.

- **802.11b Preamble**

The preamble contains information that the Array and client devices need when sending and receiving packets. All compliant 802.11b systems have to support the long preamble. A short preamble improves the efficiency of a network's throughput when transmitting special data, such as voice, VoIP (Voice-over IP) and streaming video.

Select **Auto** to instruct the Array to manage the preamble (long and short) automatically, or choose **Long Only**.

After completing all of the desired fields in the 802.11b/g Settings window, either click on the **Apply** button to save this policy or click on one of the following buttons to configure more RF policy options:

- **802.11n Settings**
Configure settings for the 802.11n wireless technology.
- **LED Settings**
Configure the activity parameters and behavior of Array LEDs.

802.11n Settings

This window establishes global 802.11n IAP settings. These settings include enabling/disabling 802.11n mode, parameters that affect performance, and defining the basic 802.11n data rates and which 802.11n data rates are supported. Any configuration parameters you set here will affect all 802.11n IAPs on the Arrays to which this policy is assigned.

For a detailed discussion of all IEEE 802.11n features such as TX and RX chains and channel bonding, please see “IEEE 802.11n Deployment Considerations” in the *Xirrus Wi-Fi Array User’s Guide*.

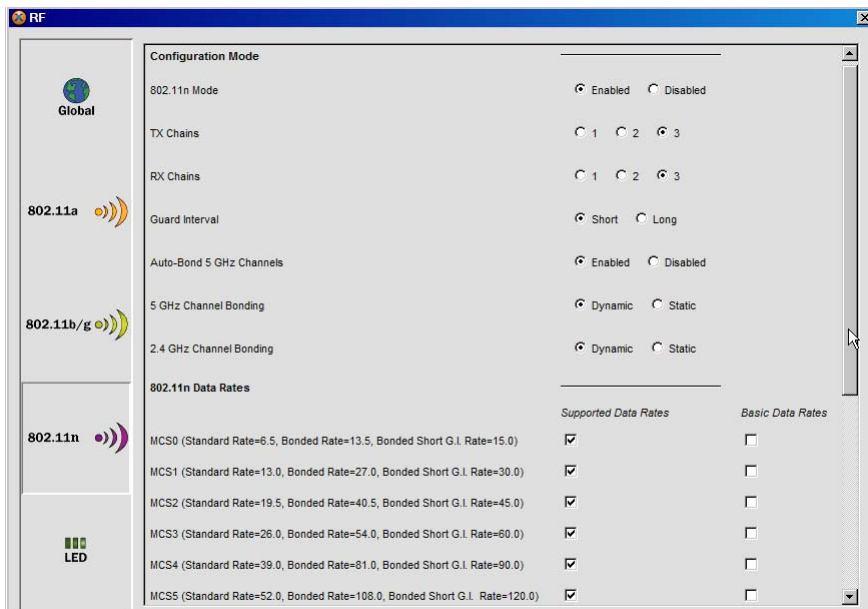


Figure 211. 802.11n RF Settings

802.11n Configuration Mode Details

- **802.11n Mode**

Select **Enabled** to operate in 802.11n mode, with four 802.11b/g/n mode ports and the remaining IAPs operating in 802.11a/n mode. The default is **Enabled**. Use of this mode is controlled by the Array’s license key. The key must include 802.11n capability, or you will not be able to enable this

mode. See the *Xirrus Wi-Fi Array User's Guide* to view the features supported by an Array's license key. Contact Xirrus Customer support for questions about your licenses.

If you select **Disabled**, then 802.11n operation is disabled on the Array. IAPs abgn1 through abgn4 will behave in the same way as IAPs abg1 to abg4 on XS Array models; the 802.11a/n IAPs will operate in 802.11a mode.

- **TX Chains**

Select the number of separate data streams transmitted by the antennas of each IAP. The default is 3.

- **RX Chains**

Select the number of separate data streams received by the antennas of each IAP. This number should be greater than or equal to **TX Chains**. The default is 3.

- **Guard interval**

Select **Short** to increase the data transmission rate by decreasing wait intervals in signal transmission. Select **Long** to use the standard interval. The default is **Short**.

- **Auto bond 5 GHz channels**

Select **Enabled** to use Channel Bonding on 5 GHz channels and automatically select the best channels for bonding. The default is **Enabled**.

- **5 GHz channel bonding**

Select **Dynamic** to have auto-configuration for bonded 5 GHz channels be automatically updated as conditions change. Select **Static** to have the bonded channels remain the same once they are selected. The Dynamic option is only available when **Auto bond 5 GHz channels** is enabled. The default is **Dynamic**.

- **2.4 GHz channel bonding**

Select **Dynamic** to have auto-configuration for bonded 2.4 GHz channels be automatically updated as conditions change. Select **Static** to have the bonded channels remain the same once they are selected. The default is **Dynamic**.

802.11n Data Rates

- **Supported Data Rates**

The data rates that are enabled here are the 802.11n data rates that your Arrays will use for transmissions to clients on the network. Check or uncheck the boxes to define which data rates are supported. The default is for all of the listed 802.11n data rates to be supported.

- **Basic Data Rates**

The data rates that are enabled here define the minimum set of 802.11n data rates that a wireless station must support if it wants to associate with the Arrays. Check or uncheck the boxes to define the basic data rates required by an 802.11n client.

After completing all of the desired fields in the 802.11n Settings window, either click on the **Apply** button to save this policy or click on the **LED Settings** button to configure more RF policy options.

LED Settings

This window allows you to disable LED activity, define which event triggers the LEDs (either when an IAP is enabled or when a station first associates with the network), and set up the behavior pattern of the LEDs on your Arrays. Any configuration parameters you establish here will affect the LED behavior on all Arrays when this policy is assigned.

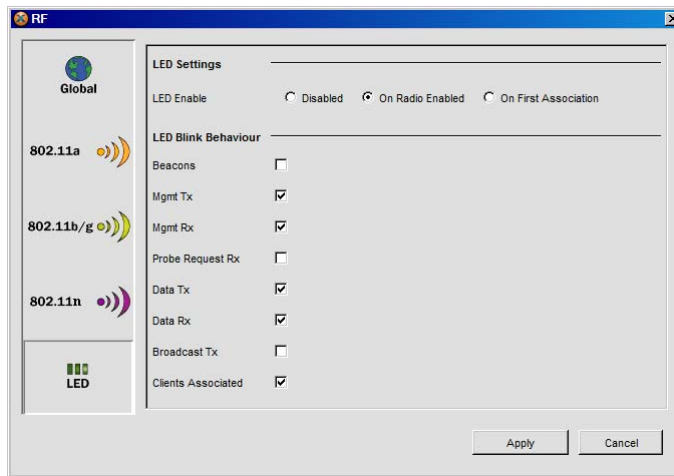


Figure 212. LED Settings

Refer to [Figure 206](#) to see where the LEDs are located on an XN16, XS16, or XS-3900 Array, which has 16 IAPs. The XN12 or XS12 Array has 12 IAPs; the XN8, XS8 or XS-3700 Array has 8 IAPs; and the XN4, XS4, or XS-3500 Array has 4 IAPs. All Array models have system and link status LEDs.

LED Setting Details

- **LED Enable**

This option allows you to enable or disable the IAP LEDs (not the system or link status LEDs), and determines which event triggers the LED sequencing—either when an IAP is enabled or when an IAP first associates with the network. Choose **On Radio Enabled** or **On First Association**, as desired.

LED Blink Behaviour

- **All Activities**

These options allow you to select when the IAP LEDs blink, based on the activities you check here. From the choices available, select one or more activities to trigger when the LEDs blink. The default is to have the following activities enabled:

- Mgmt Tx
- Mgmt Rx
- Data Tx
- Data Rx
- Clients Associated

Saving Your RF Policy

When you have configured all of your RF policy settings, click on the **Apply** button in the RF Settings window to save the new policy.

WDS

Open the **Configuration > Policies** node in the **Tree**, and select **WDS** to display the WDS policy window. The WDS (Wireless Distributed System) enables the interconnection of access points wirelessly, allowing your wireless network to be expanded using multiple Arrays without the need for a wired backbone to link them.

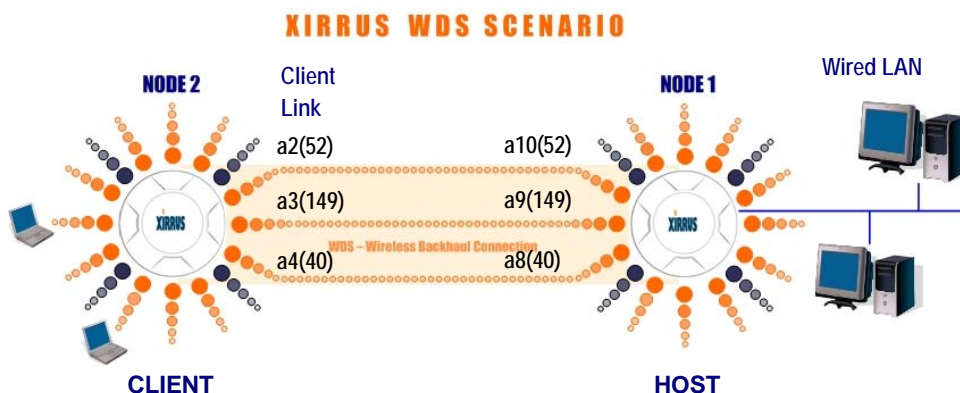


Figure 213. Configuring a WDS Link

The WDS policies allow you to set up configuration for WDS networks. Note that when you apply a WDS policy to an Array, the policy replaces any prior WDS configuration. Any pre-existing WDS setup on the Array will be lost.

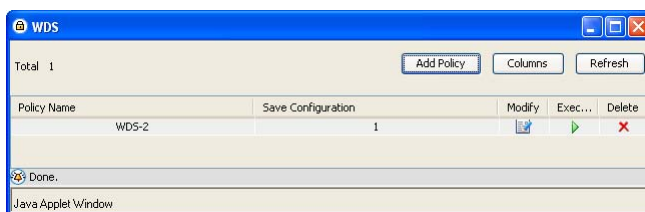


Figure 214. WDS Policy Window

The columns in the WDS policy window show selected settings for the listed policies. For information about changing the columns displayed, see **“Selecting the Columns Shown in a Policy Window” on page 220**.

About Configuring WDS Links

A WDS link connects a client Array and a host Array (see [Figure 213](#)). The host must be the Array that has a wired connection to the LAN. Client links from one or more Arrays may be connected to the host, and the host may also have client links.

The configuration for WDS is performed on the client Array only, as described in [“WDS Client Links” on page 344](#). No WDS configuration is performed on the host Array. First you will set up a client link, defining the target (host) Array and SSID, and the maximum number of IAPs in the link. Then you will select the IAPs to be used in the link. When the client link is created, each member IAP will associate to an IAP on the host Array.

For more information on WDS and how to use it, see the discussion in the *Xirrus Wi-Fi Array User’s Guide*.

Creating a WDS Policy

To create a new WDS policy, click **Add Policy** in the WDS Policy window. When the Add Policy window appears, select **Copy from a chosen Array (recommended)** and choose a model Array, or select **Start from scratch**, as described in [“Adding a Policy” on page 219](#). Click **OK**. The WDS policy details window appears. It is divided into two primary areas:

- **WDS Client Links**

This section defines the policy name and sets up the link on the Array, but doesn’t actually assign any IAPs to the link.

- **WDS Client IAP**

Use this section to assign IAPs to links.

WDS Client Links

The WDS Client Links window names a WDS policy and configures one or more of the four WDS links that are available for configuration on each Array.

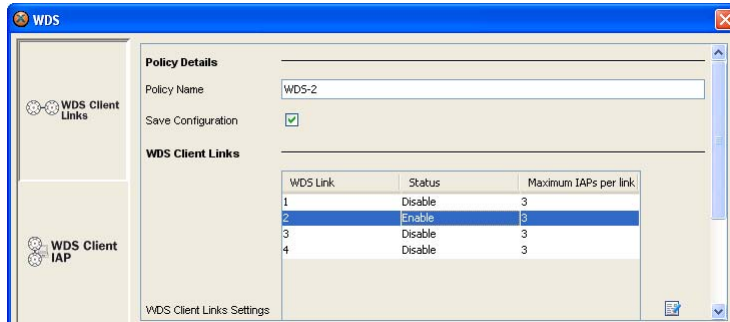


Figure 215. WDS Client Links

Enter the **WDS Policy Name**, and select an entry from the **WDS Client Links** list to configure. Click the check box to the right of the list, and the **WDS Client Links Settings** window will appear for the selected link. Configure it as described below. You may repeat the procedure to configure up to all four links. Click **Apply** when done to save the policy.

WDS Client Links Settings

Use this window to configure the target of a selected WDS link (i.e., specify the far end Array and SSID).

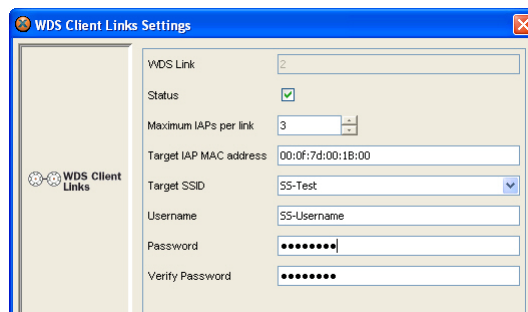


Figure 216. WDS Client Link Settings

WDS Client Links Setting Details

- **WDS Link**
The WDS Link will be grayed out since this is the link that you chose on the previous screen.
- **Status**
Enable or Disable the WDS Link
- **Maximum IAPs per Link**
Choose the number of radios that you wish to use for the WDS link. This setting is used to allow more bandwidth if the WDS Link is over loaded.
- **Target IAP MAC address**
Enter the base MAC address of the target Array (the host Array at the other side of this link). This address is the base address of the target Array's IAP MAC Range. To display this address, use the Web Management Interface on the target Array ("[Connecting to an Array](#)" on [page 172](#)), and log in. Click **WDS**, and look for **This Array Address** at the bottom of the window. Alternatively, click **Array Info** and look for **IAP MAC Range**, then use the starting address of this range.
- **Target SSID**
Enter the SSID used for the WDS Link.
- **Username**
Enter the user name used for security on your Array if it is enabled.
- **Password, Verify Password**
Enter the password used for security on your Array if it is enabled, and then re-enter it in the **Verify Password** field to confirm it.

WDS Client IAP

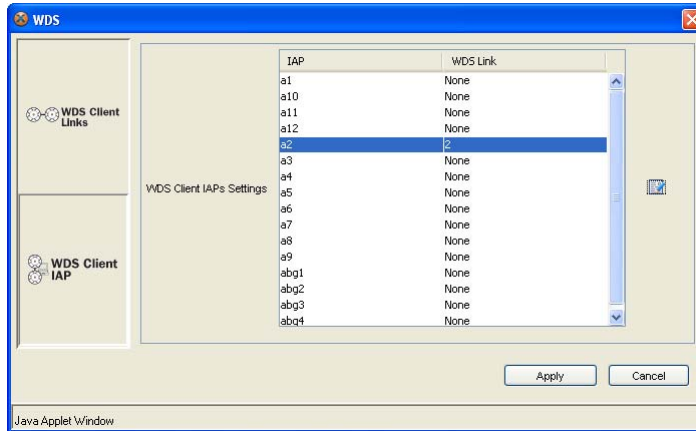


Figure 217. WDS Client IAP Window

Click **WDS Client IAP** on the left side of the screen to select the radios that are part of the WDS Link. The **WDS Client IAP Window** is displayed (**Figure 217**). You can assign radios to WDS Links 1 to 4.



Once an IAP has been selected to act as a WDS client link, you will not be allowed to use auto-configured cell sizing on that IAP (since the cell must extend all the way to the other Array).

Double-click on an IAP that you wish to assign to a WDS link. The **WDS Client IAP Settings** dialog box appears. (**Figure 218**)

WDS Client IAP Settings

- **IAP**

This is the radio that was selected for the WDS Link. It cannot be modified.

- **WDS Link**

Choose one of the four WDS Link numbers from the drop down box. The IAP will be assigned to this WDS link.

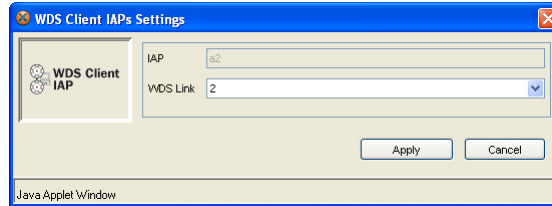


Figure 218. WDS - Assign IAP to Client

Saving Your WDS Policy

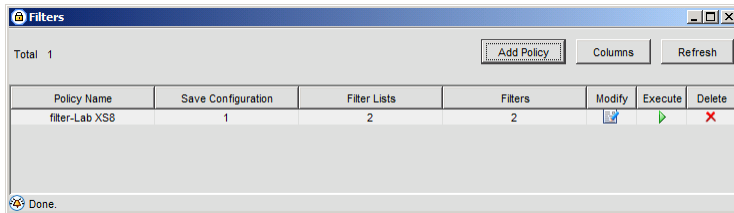
When you have configured all of your WDS policy settings, click on the **Apply** button in the WDS window to save the new policy.

Filters

The Wi-Fi Array’s integrated firewall uses stateful inspection to speed the decision of whether to allow or deny traffic. Filters are used to define the rules used for blocking or passing traffic on the Array. Filters can also set the VLAN and QoS level for selected traffic. Filters are organized on the Array in groups, called **Filter Lists**. A filter list allows you to easily apply a uniform set of filters to **SSIDs** or **User Groups**.

User connections managed by the Array’s firewall are maintained statefully—once a user flow is established through the Array, it is recognized and passed through without application of all defined filtering rules. Stateful inspection runs automatically on the Array. Policies may be configured to manage filters.

From the **Configuration>Policies** node in the tree, click on **Filters** to display the Filters window. This window contains the a list of all the filter policies currently available, with tools to manage these policies.






Policy Name	Save Configuration	Filter Lists	Filters	Modify	Execute	Delete
filter-Lab XSS	1	2	2			

Figure 219. List of Filter Policies

The columns in this window show selected settings for the listed policies. For information about changing the columns displayed, see **“Selecting the Columns Shown in a Policy Window” on page 220**.

Creating a New Filter Policy

A filter policy allows you to configure all of the desired filters on an Array at the same time, allowing or denying protocols, source addresses, and VLANs.

You must first create one or more filter lists in a filter policy. Then select a filter list and create and manage all the filters that are members of that filter list.

To create a new filter policy click on the **Add Policy** button in the Filter Policy window. When the Add Policy window appears, select **Copy from a chosen Array (recommended)** and choose a model Array, or select **Start from scratch**, as described in **“Adding a Policy” on page 219**. Click **OK**. The Filters policy details window appears.

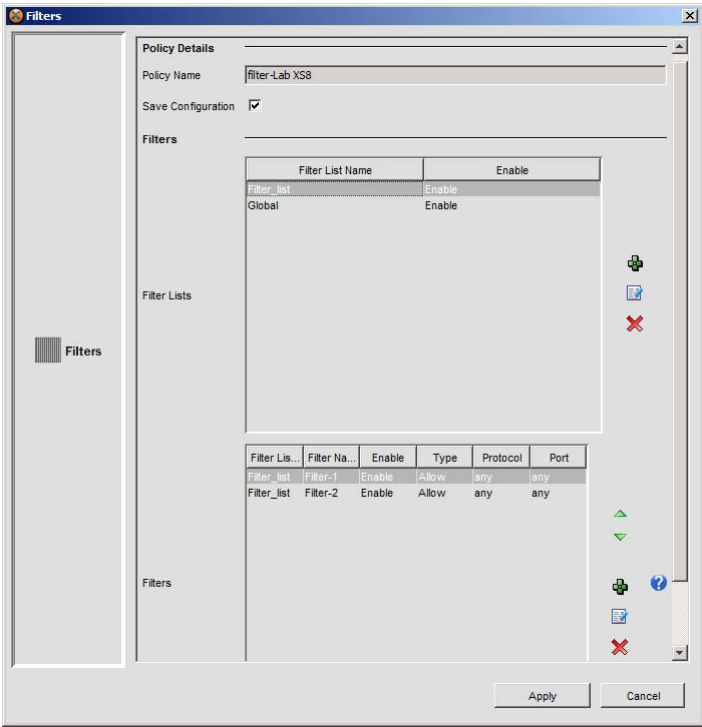


Figure 220. Filter Policy Details

Note that each Array comes with one predefined filter list, named **Global**, which cannot be deleted. Filter lists (including Global) may be applied to SSIDs or to User Groups. Only one filter list at a time may be applied to a group or SSID (although the filter list may contain a number of filters). All filters are created within filter lists.

Policy Details

- **Policy Name**

Enter a meaningful name that describes this policy. If you are modifying an existing policy this field is grayed out (not editable). If you are using a standard naming convention for all of your policies, the name you enter here should conform to that convention.

- **Save Configuration**

Check this box to ensure that any time this policy is applied to an Array, the Array will save the updated configuration information to its flash memory. If this box is left unchecked, then when this policy is applied to Arrays the configuration changes will need to be saved manually or else they will be lost when the Arrays are rebooted. Note that this checkbox does not actually apply the policy to any Arrays. To apply the policy, see **“Using Policy Windows” on page 218**.




The remainder of the Filter Policy window has two main boxes:

- **Filter Lists**
- **Filters**

Filter List Details

- **Filter Lists**

The Filter List box shows a list of any previously created filter lists. XMS has a default filter list, **Global**. This default list is always present, although it may not be listed. When you select a filter list entry, the **Filters** box will show the filters defined for the selected list.

New filter lists may be added by pressing the  button to the right of the list and filling in the fields shown below; existing entries may be edited by pressing the  button and deleted by pressing the  button.

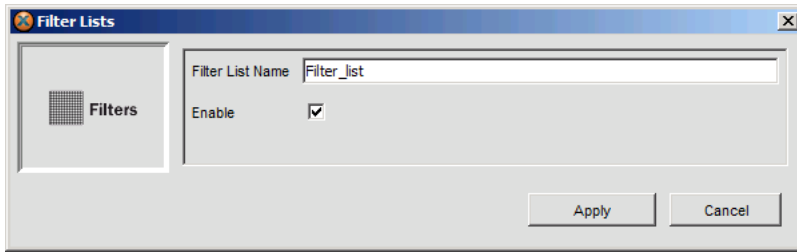


Figure 221. Filter List Details

Filter List Setting Details


- **Filter List Name**
Enter a meaningful name for the filter list.
- **Enable**
Check this box if you wish to enable this filter list.



Filters

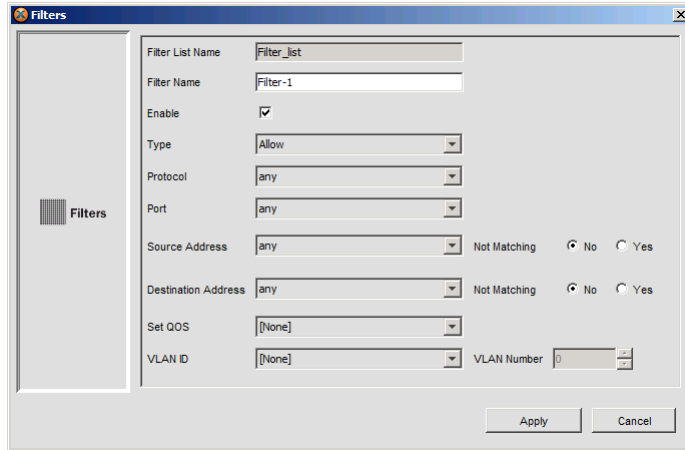
NOTE: We recommend that you configure VLAN settings before creating a new Allow filter.

- **Filters**
This is the area in which you create and manage the individual filters. Select a filter list entry, and the Filters box will show any filters already created for that list. When a filter list is used by an SSID or user group on an Array, the filters in that list are executed in order: the first entry (at the top of the list) is executed first, followed by the second, and so on. You can use the up and down arrows to change the order of the filters in the list.

Note that filtering is secondary to the stateful inspection performed by the Array's integrated firewall. Traffic for established connections is passed through without the application of these filtering rules.

Filters may be added to the list by pressing the  button to the right of the Filters box and filling in the fields described in [Filter Details](#) below. Note that if you have not selected a filter list, then this filter will be added

to the default filter list, named Global. Existing filter entries may be edited by pressing the  button and deleted by pressing the  button.



The dialog box titled "Filters" contains the following fields and controls:

- Filter List Name:** Filter_list
- Filter Name:** Filter-1
- Enable:** ☒
- Type:** Allow
- Protocol:** any
- Port:** any
- Source Address:** any, Not Matching: ☒ No, ☐ Yes
- Destination Address:** any, Not Matching: ☒ No, ☐ Yes
- Set QOS:** [None]
- VLAN ID:** [None], **VLAN Number:** 0

Buttons: Apply, Cancel

Figure 222. Filters Setting Details

Filter Details

- Filter List Name**
 This read-only field shows the name of the filter list to which this filter belongs.
- Filter Name**
 Enter a meaningful name for the filter.
- Enable**
 Check this box if you wish to enable the filter when you execute the list.
- Type**
 Choose whether to **Allow** or **Deny** packets that meet the specifications on this page.
- Protocol**
 Choose the protocol that you wish to allow or deny from the drop down box. The available protocols are **any-ip**, **icmp**, **igmp**, **srp**, **tcp**, **udp**, **arp**. Choose **any** to match all protocols.

- **Port**
Choose the port that you wish to block. The available ports are **echo**, **discard**, **daytime**, **chargen**, **ftp-data**, **ftp**, **ssh**. Choose **any** to match all ports.
- **Source Address**
Select the type of the source address for the machine that you wish to allow or deny—**Group**, **IP**, **SSID**, **VLAN**, **MAC**, or **Interface**. The next fields will be changed to accommodate the type of address that you selected., for example, IP Address and Mask, VLAN, MAC and Mask, etc. Choose **any** to match all addresses.

Click **Yes** to apply the filter to all traffic matching the **Source Address**, or **No** to apply the filter to all traffic not matching the criteria.
- **Destination Address**
Select the type of the destination address for the machine that you wish to allow or deny—**Group**, **IP**, **SSID**, **VLAN**, **MAC**, or **Interface**. The next fields will be changed to accommodate the type of address that you selected., for example, IP Address and Mask, VLAN, MAC and Mask, etc. Choose **any** to match all addresses.

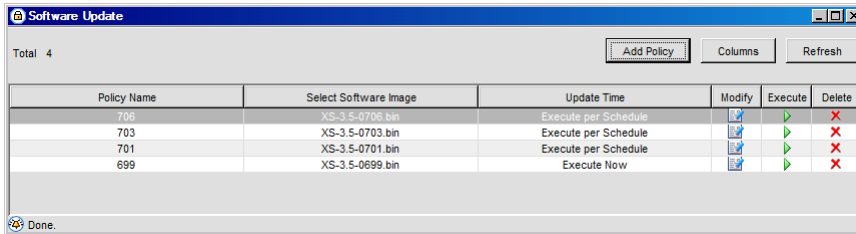
Click **Yes** to apply the filter to all traffic matching the **Destination Address**, or **No** to apply the filter to all traffic not matching the criteria.
- **Set QOS**
Choose the QOS (Quality of Service) value of an allowed packet, from 0-3. Level 0 has the lowest priority; level 3 has the highest priority. This field is grayed out when **Type** is set to **Deny**.
- **VLAN**
Set the **VLAN ID** and the **VLAN Number** of an allowed packet. These fields are grayed out when **Type** is set to **Deny**.

Saving Your Filter Policy

When you have configured all of your filter policy settings, click on the **Apply** button in the Filter policy window to save the new policy.

Software Update

From the **Configuration>Policies** node in the tree, click on **Software Update** to display the Software Update window. This window contains a list of all software update policies currently available, with tools to manage these policies.















Policy Name	Select Software Image	Update Time	Modify	Execute	Delete
706	XS-3.5-0706.bin	Execute per Schedule			
703	XS-3.5-0703.bin	Execute per Schedule			
701	XS-3.5-0701.bin	Execute per Schedule			
699	XS-3.5-0699.bin	Execute Now			

Figure 223. List of Software Policies

The columns in this window show selected settings for the listed policies. For information about changing the columns displayed, see [“Selecting the Columns Shown in a Policy Window” on page 220](#).

Creating a New Software Update Policy

A software update policy is created so that you can set up the file transfer parameters for the new software image and schedule your updates. Of course, the image must first be moved to the XMS server, so that it is available for upload to Arrays. The policy has a tool for downloading images onto the server.

To create a new update policy, click on the **Add Policy** button in the Software Update window. The Software Update window is displayed, which is divided into three primary areas:

- **File Details**
Allows you to define the image file and file transfer information.
- **Custom Login**
Allows you to set up authentication parameters for access to the Array.
- **Schedule Details**
Allows you to schedule when your software update is performed, and define whether or not the Arrays are automatically rebooted when the update process is complete.

File Settings

This window contains fields for defining the name of the policy and configuring the software update image file transfer process.

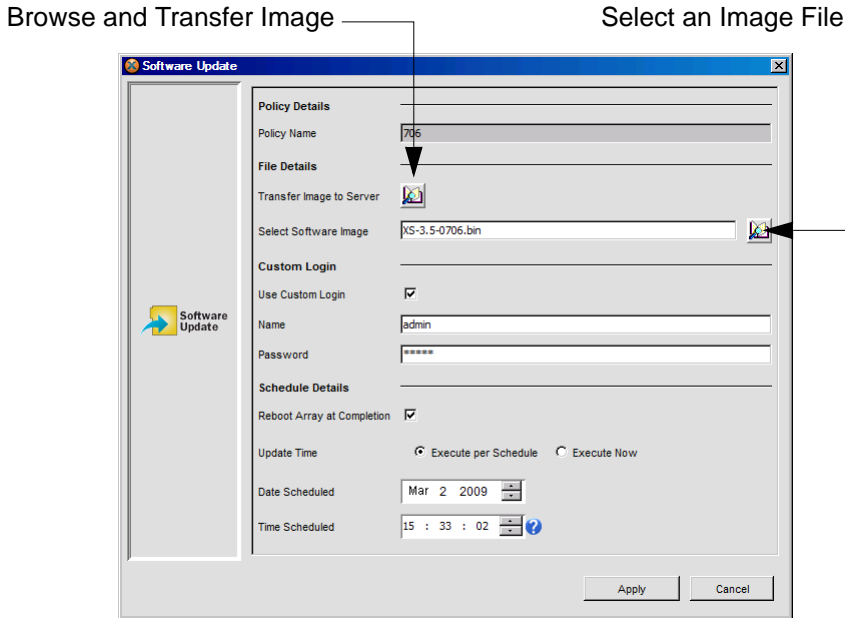


Figure 224. Software Update

Policy Details

- **Policy Name**

Enter a meaningful name that describes this policy. If you are modifying an existing policy this field is grayed out (not editable). If you are using a standard naming convention for all of your policies, the name you enter here should conform to that convention.

File Details

- **Transfer Image to Server**

Click this button ([Figure 224](#)) to browse for the Array image file and transfer the file to the XMS database.

- **Select Software Image**

Click this button ([Figure 224](#)) to browse for the image file from the File Chooser window, then select the file.

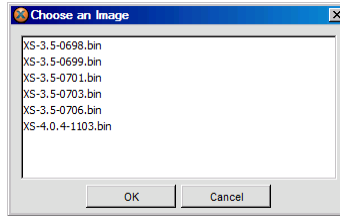


Figure 225. File Chooser

Custom Login

- **Use Custom Login**

Custom Login is optional if SNMP is enabled on the device and it is running an ArrayOS release greater than 3.5.

Check this box and set up the login parameters required for uploading the image to Arrays. The upload uses Secure Channel Protocol (SCP) to authenticate access to each Array. The Array will accept logins that match any of its **Admin** accounts with write privileges. These accounts may be entered either directly on the Array or using **Management Control** policies. Also, this process will use any Array Shell Authentication information defined in the discovery dialog (see **“Adding or Deleting Array Shell Authentication Entries” on page 80**). Note that Arrays are shipped with the factory default login **admin/admin**.

- **Name/Password**

Enter a name and password for access to an Array. These values must match an admin account that is configured on the Array, else the upload to the Array will fail.

Schedule Details

- **Reboot Array at Completion**

Check this box if you want to reboot the Arrays when the software update process is complete. The default is for this box to be checked.

The updated software will not become the running image on the Arrays until they have been rebooted.

- **Update Time**

Select whether the update is to be performed at a scheduled time, configured below, or whether the update is to be performed immediately. **Execute Now** is the default.

- **Date Scheduled**

Enter a date for the update, or click in a field (month/day/year) and increment/decrement the values using the UP and DOWN arrows. This option is only applicable if you chose **Execute per Schedule** in the Periodicity field, otherwise this option is grayed out.

- **Time Scheduled**

Enter a time for the update, or click in a field (hour/minute/second) and increment/decrement the values using the UP and DOWN arrows. This option is only applicable if you chose **Execute per Schedule** in the Periodicity field, otherwise this option is grayed out.

Saving Your Software Update Policy

When you have configured all image file transfer and scheduling settings for your updates, click **Apply** in the Software Update window to save the new policy.

Web Page Redirect (WPR)

From the **Configuration>Policies** node in the tree, click on **Web Page Redirect** to display the Web Page Redirect window. This window contains a list of all WPR policies currently available and the number of files to be uploaded by each, with tools to manage these policies.

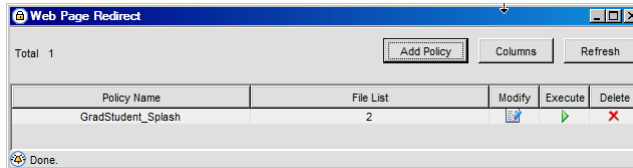


Figure 226. List of WPR Policies

Creating a New Web Page Redirect Policy

A Web Page Redirect policy is created so that you can set up the transfer of custom WPR files to Arrays. Of course, the files must first be moved to the XMS server, so that they are available for upload to Arrays. The WPR policy has a tool for downloading these files onto the server.

To create a new WPR policy, click **Add Policy** in the WPR window. The Web Page Redirect policy details window is displayed. (Figure 227)

Download a File to XMS Server

Add Files to Be Transferred

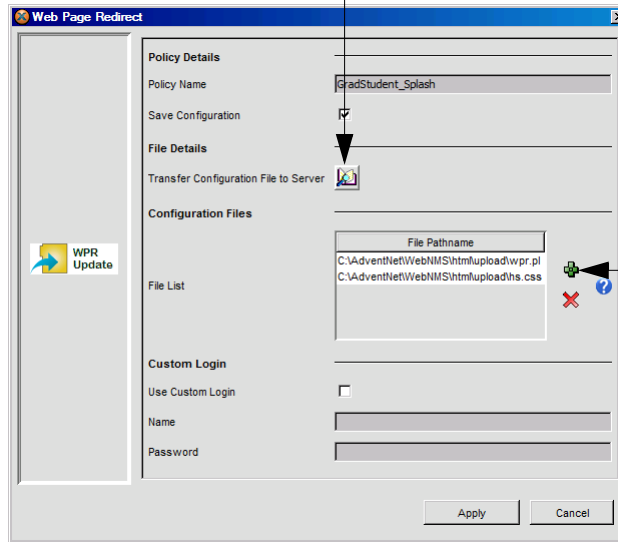


Figure 227. Web Page Redirect

Policy Details

- **Policy Name**

Enter a meaningful name that describes this policy. If you are modifying an existing policy this field is grayed out (not editable). If you are using a standard naming convention for all of your policies, the name you enter here should conform to that convention.

- **Save Configuration**

Check this box to ensure that any time this policy is applied to an Array, the Array will save the updated configuration information to its flash memory. If this box is left unchecked, then when this policy is applied to Arrays the configuration changes will need to be saved manually or else they will be lost when the Arrays are rebooted. Note that this checkbox does not actually apply the policy to any Arrays. To apply the policy, see [“Using Policy Windows” on page 218](#).

The remainder of the WPR Policy window has three main sections:

- **File Details**
Downloads the custom WPR files onto the XMS server, so that they will be available for transfer to Arrays when you execute the policy.
- **Configuration File Details**
Allows you to define the custom WPR files to be uploaded to the Arrays.
- **Custom Login Details**
Specifies the login parameters necessary for authentication on Arrays, so that the Arrays will permit the XMS server to proceed with uploading the custom WPR files.

File Details

This section contains a button for downloading custom WPR files to the XMS server. The files will then be available for upload to Arrays.

- **Transfer Configuration File to Server**
Click on the browse button to browse for a custom WPR file from the Upload window, then select the file. The file will be transferred to the appropriate folder on the XMS server.

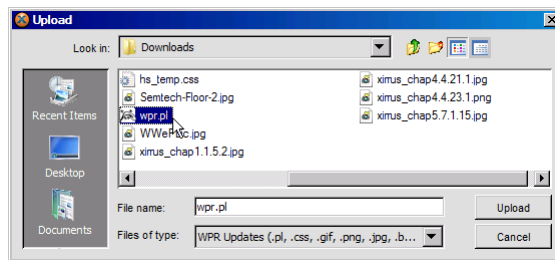




Figure 228. WPR File Upload to XMS Server

Configuration File Details

- **File List**
This section allows you to create a list of the custom WPR files to be uploaded to an Array when this policy is executed. Files may be added to the list by pressing the  button to the right of the File List box. The WPR

dialog box (**Figure 229**) lists the files that you have downloaded to the XMS server for this purpose. Select a file to be added to the File List and click **Add**.

Existing File List entries may be deleted by pressing the  button.

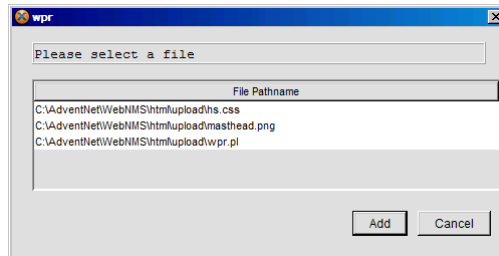


Figure 229. Selecting WPR File List Entries

Custom Login Details

- **Use Custom Login (Required)**

You must check this box and set up login parameters for uploading the custom WPR files to Arrays. The upload uses Secure Channel Protocol (SCP) to authenticate access to each Array. The Array will accept logins that match any of its **Admin** accounts with write privileges. These accounts may be entered either directly on the Array or using **Management Control** policies. Note that Arrays are shipped with the factory default login **admin/admin**.

- **Name/Password**

Enter a name and password for access to an Array. These values must match an admin account that is configured on the Array, else the upload to the Array will fail.

Saving Your Web Page Redirect Policy

When you have configured all file transfer and login settings for your custom WPR files, click **Apply** in the Web Page Redirect window to save the new policy.

Configuration File (Advanced)

From the **Configuration>Policies** node in the tree, click on **Config File (Advanced)** to display the Config File window. This window contains a list of all config file policies currently available, with tools to manage these policies.

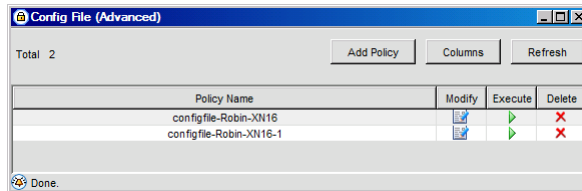


Figure 230. List of Config File Policies

The columns in this window show selected settings for the listed policies. For information about changing the columns displayed, see **“Selecting the Columns Shown in a Policy Window” on page 220**.

Creating a New Config File Policy

A Config File policy is used to apply a configuration file to Arrays. The file may be copied from the existing configuration of an Array that you select as a model, or may be typed in from scratch. For example, if Xirrus Customer Support sends you a config file, you may start from scratch and copy the file and paste it in.



*This policy is intended for **advanced users** who are familiar with use of the Xirrus Wi-Fi Array CLI and configuration files. Only **expert users** should use the option to create a configuration file from scratch.*

Config file policies are useful in a number of situations. In particular, they are the *only* way to apply new features to Arrays before those features have been incorporated in XMS.

A config file policy has the following abilities:

- CLI commands may be used to push a configuration to Arrays. An Array configuration file is really just a series of CLI commands.
- You may base the policy on the existing configuration of a selected Array.

- Partial configurations may be pushed to Arrays—that is, you may edit the configuration file to contain only the settings that you wish to change on Arrays. The file makes incremental changes to the settings on an Array when the policy is executed. Thus, *settings not defined in the config file will be left unchanged*.

To create a new config file policy, click **Add Policy** in the Config File window. When the Add Policy window appears, we strongly recommend that you select **Copy from a chosen Array** to fetch the configuration from one of the Arrays shown in the list. (Figure 231) Only *expert* users should use **Start from scratch**! (See “Adding a Policy” on page 219.) Click **OK**. The policy details window appears.

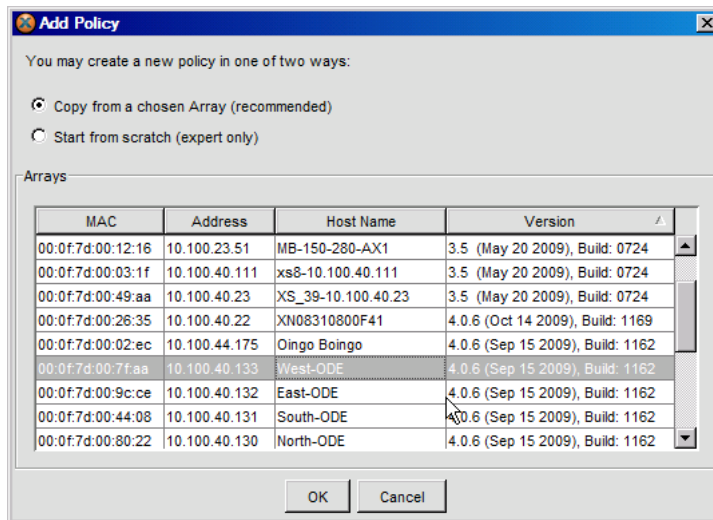


Figure 231. Create Config File Policy

Policy Details

- Policy Name**
If you copied the policy from an Array, then the Array’s Host Name is used as the Policy Name by default—this name may be edited if you wish. Otherwise, enter a meaningful name for this policy. If you are modifying an existing policy this field is grayed out (not editable). If you

are using a standard naming convention for all of your policies, the name you enter here should conform to that convention.

- **Config File**

This section allows you to edit the configuration file that will be uploaded to Arrays when this policy is executed. (Figure 232) If you used **Copy from a chosen Array**, the configuration file that was fetched from the selected Array is displayed. If you selected **Start from scratch**, then the text area will be empty and you can enter the CLI commands that you wish to apply to Arrays.

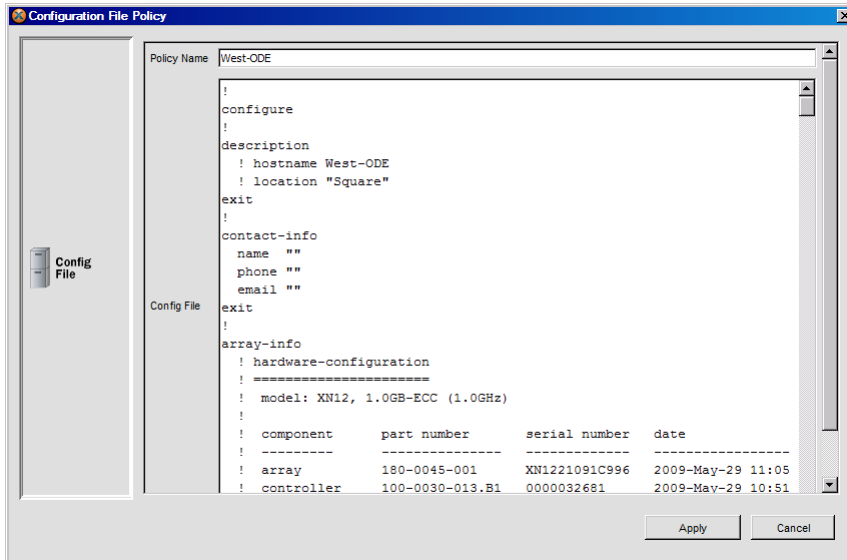


Figure 232. Configuration File Edit and View Window

About a Config File Copied from an Array

When you fetch a config file from an Array, the file represents the entire configuration of the Array, except that XMS makes certain modifications to the file for your convenience:

- The IAPs will be reset and then will all be brought back up. Similarly, other settings such as SSID, User Group, DHCP Server, and VLAN will be reset and brought back up.

- All other radio (IAP) settings are commented out, so that no radio settings will change. Certain other settings, such as Hostname, Location, and ArrayOS primary and backup software images will be commented out as well in order to prevent these device-specific settings from being applied to multiple Arrays.

Editing the Configuration File

You may type text to enter it in the box, and use the **Backspace** and **Delete** keys. You cannot search for text, but you can use common selection and cut and paste keys:

- Ctrl+a: Select all
- Ctrl+c: copy selected text
- Ctrl+x: cut selected text
- Ctrl+v: paste text from buffer (may be from an application other than XMS)
- Shift+Click: select contiguous text up to clicked location
- Shift+Arrow: select contiguous text in direction of arrow

Saving Your Config File Policy

When you have finished any desired edits to the configuration file, click **Apply** to save the policy.

Groups

From the Configuration menu, click on **Groups** to display the Groups window. This window contains a list of all Array groups currently available, with tools to manage these groups, including the ability to apply a set of policies to the Arrays in the group. This allows you to apply a uniform configuration to all of the members in one step. Array groups are also useful for filtering the data shown in the Dashboard and other windows, as described in [“About Dashboard Data” on page 92](#).

Array ...	Array ...	Global...	Syste...	Manag...	Network	Services	VLAN	DHCP...	Security	SSIDs	User G...	IAPs	RF	WDS	Filters	Modify	Execute	Delete
test	1	None	None	None	None	None	None	None	None	None	None	None	None	None	None			

Figure 233. List of Groups

The columns in this window show selected settings for the listed policies. For information about changing the columns displayed, see [“Selecting the Columns Shown in a Policy Window” on page 220](#).

Creating A New Group

An Array group is created so that you can define groups of Arrays and apply policies to the group. To create a new Array group, click on the **Add Group** button in the Groups window. The Array Group Settings window is displayed, which is divided into two primary areas:

- **Array Group Settings**
Allows you to define a group name and assign Arrays to the group.
- **Policy Details**
Allows you to assign **Global Policy Settings** to the Array group.

Array Group Settings

This window contains a field for assigning the group name, and a list of Arrays that can be assigned to the group.

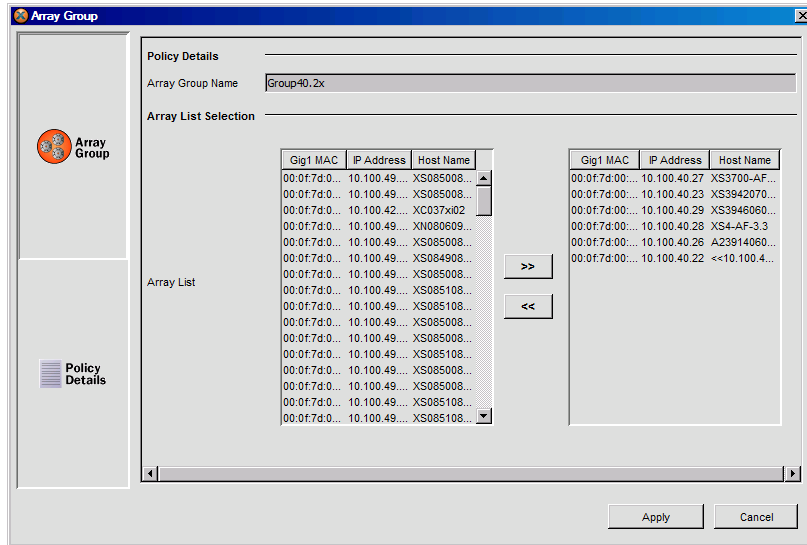


Figure 234. Array Group

Policy Details

- **Array Group Name**
Enter a meaningful name that describes this Array group.

Array List Selection

- **Array List**
To add an Array to this group, click on an Array in the left column then click on the >> button to move the Array to the right (include) column. To remove an Array from the group, click on an Array in the right column then click on the << button to move the Array to the left (exclude) column.

Policy Details

This window allows you to select policies to be applied to the Arrays in the group. It is very similar to the [Global Policy Settings](#) window, and contains fields for selecting the policies to be applied to the group.

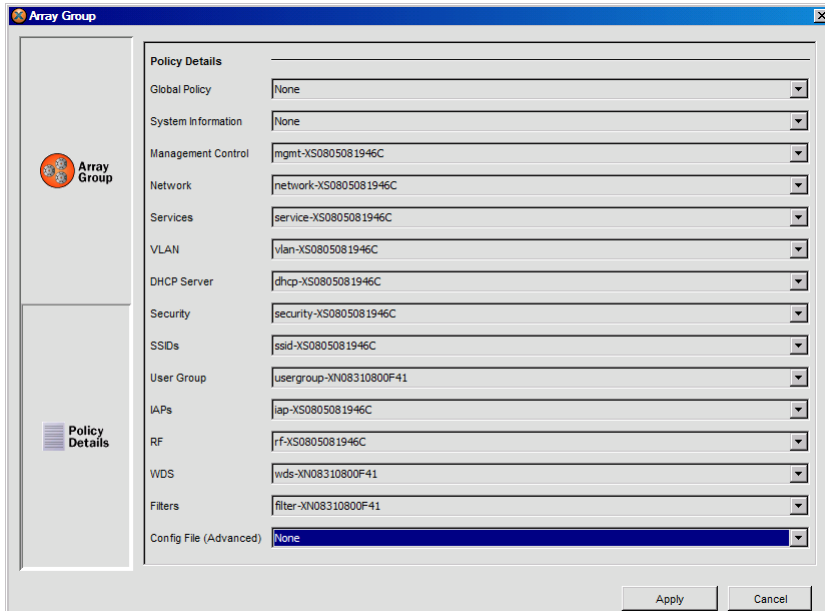


Figure 235. Policy Details

- **All Policy Types**

Choose a policy from the pull-down list for the Global Policy, or choose a policy for some or all of the policy types listed in this window. The policies you choose here will be applied to the group when you click **Apply**. Select **None** for each category of configuration that you want to leave as-is on the Arrays.

You may select a Global Policy to apply—this applies all of the policies that are included in the Global Policy. If you select a Global Policy, you may not select any other types of policies - the rest of the window will be disabled.

If you do not select a Global Policy, then you may select policies for some or all of the other policy types (only one policy may be selected for each policy type).

Applying Your Array Groups Policy

When finished, click on the **Apply** button in the Array Groups Settings window to save the new policy.

Audit

This function creates an audit trail (record) of all configuration changes that have been performed on your Arrays. To access this function, click on the Audit node in the Configuration section of the **Tree** then use either of the following procedures to review the audit details.

- Right-click on an audit item in the table and choose **Details** from the pull-down list.
- Select an audit item in the table, then go to the **Menu Bar** and choose **View > Details**.

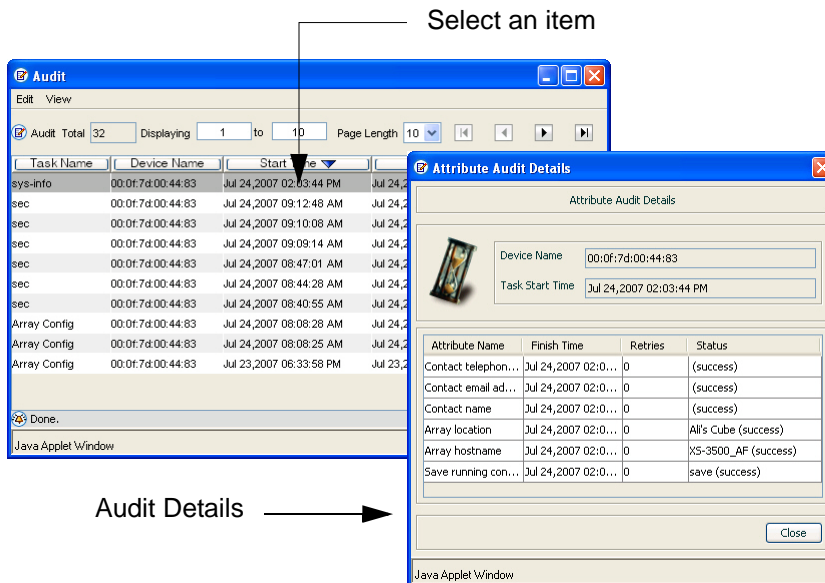


Figure 236. Viewing the Audit Details

Managing Reports

XMS generates performance reports about the network, all Wi-Fi Arrays within the network, the individual IAPs (Integrated Access Points) contained within each Array, and wireless data (channels, throughput, signal strength, etc.). Selection criteria allow you to focus your reports on just the data that is of interest.



Click the **Reports** button in the main menu at the top of the page to access the reports pages.

This chapter provides instructions for managing and reviewing these reports via the web client. Section headings for this chapter include:

- [“About Reports” on page 371](#)
- [“Traffic Reports” on page 388](#)
- [“Station Reports” on page 404](#)
- [“Array Reports” on page 412](#)
- [“RF Reports” on page 416](#)
- [“Security Reports” on page 419](#)

About Reports

Reports provide information about the content, performance and usage of your network(s) and Arrays. Most reports display a combination of graphs and text-based information organized in tabular form.

There are three main reports pages:

- **My Reports**—The web client’s **Reports** button opens to the **My Reports** page, listing all of the reports you have already created and allowing you to view or run these reports.
- **New Report**—Click this link to list all the types of reports that you can create. Click on a report, and a form allows you to enter all the selection criteria for your report. You may then save the report setup, and run it now or schedule it for later.

- **Customize**—Click this link to customize the appearance of reports by changing the logo at the top of the report.

Selection Criteria differ according to the type of report, but most reports use similar criteria such as defining the group of Arrays and time period to consider for the report.

Reports are not to be confused with events and alarms, which provide alerts when the system encounters problems. For information about events and alarms, go to **“Monitoring Your Network” on page 105**.

Sample reports shown in this chapter may show multiple Arrays managed by XMS. In some cases you may see examples where only one Array is under management. The results are the same regardless of how many Arrays are being addressed.

Topics for this section include:

- **“My Reports” on page 373**
- **“Viewing a Report” on page 375**
- **“New Report” on page 378**
- **“Selection Criteria” on page 384**
- **“Customize” on page 387**

My Reports

To access reports, click the **Reports** button at the top of the web client window. The initial window always defaults to the **My Reports** page. If you are on one of the other Reports pages, click the **My Reports** link on the left to return to this page.

This page lists all of the reports that you have already created using the **New Report** link. You may view latest or archived report results, run the report, or edit report parameters from this page. The list of reports may be sorted by clicking on the column header for the **Report**, **Last Run**, or **Scheduled** columns. Click again to reverse the sort order.

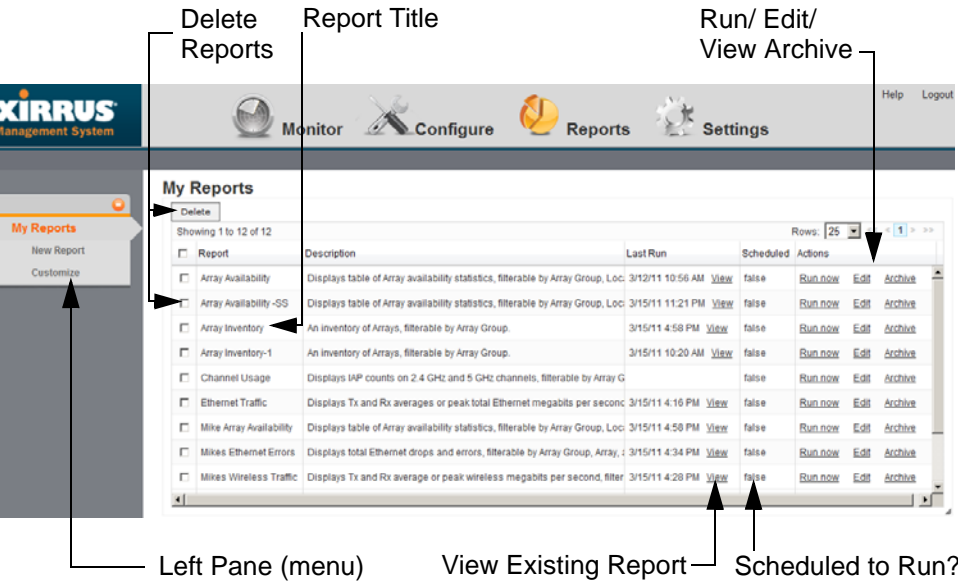
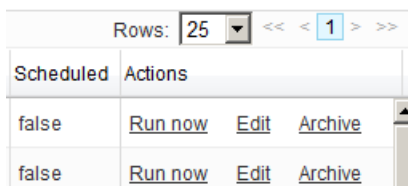


Figure 237. My Reports Window

The following information is displayed for each report:

- **Report**—this is the **Name** that you assigned when you created the report. To delete a report, select the checkbox to the left of it, then click the **Delete** button at the top left. Select as many reports as you wish for deletion. You may click the checkbox in the header row to select or deselect all reports.

- **Description**—this is a general description of this type of report.
- **Last Run**—this column lists the time that the report was most recently run, if any. Click the **View** link to see that report. For a description of the options available, see “**Viewing a Report**” on page 375).
- **Scheduled**—**true** indicates that the report has been scheduled to run at some time in the future.



Rows: 25 << < 1 > >>	
Scheduled	Actions
false	Run now Edit Archive
false	Run now Edit Archive

Figure 238. Actions for Reports

- **Actions (Figure 238)**—this column allows you run or edit this report, or see all of its saved runs.

Click **Run Now** to start a report immediately. The **Report Queue** page will be displayed, showing the status of the report. You may go to other web client pages to perform tasks while the report is generated. Generating reports may take some time on large Array networks.

Click **Edit** to change the selection criteria for the report. This displays the same fields you entered when you originally used **New Report** to create the report, as described in “**Selection Criteria**” on page 384. You may change any field, including the report’s **Name**. Note that this report will *replace* the edited report, even if you change the name (i.e., you will not have entries listed on the My Reports page for the old name and the edited name—the Archive entries that were created with the old name will still be there under the new name).

Click **Archive** to list all of the saved copies of this report. (Figure 239) Each time a report is run, it is automatically saved with a date/time stamp. The archive lists these reports in the order that they were run. Click the desired format for a report: **html**, **Excel**, **pdf**, or **csv**. You may choose to save the resulting file to your file system, or display it immediately (the appropriate software is automatically used). For

example, a CSV file is displayed by Excel. See “[Viewing a Report](#)” on [page 375](#) for more details. You may click the **Delete** link in front of a report if you wish to remove it.

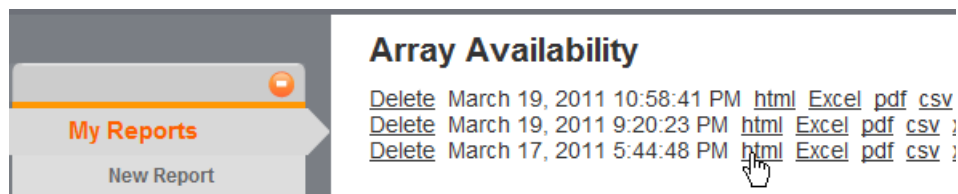


Figure 239. Archived Reports List

Viewing a Report

You may select a report for viewing from two places on the **My Reports** page:

- Click the desired report’s **View** link in the **Last Run** column. ([Figure 240](#))
- Click the desired report’s **Archive** link in the **Actions** column to choose the report with the desired time stamp. Click the **html** link to view the report as shown in [Figure 239](#).

When you create and run a report from the **New Report** page, it is automatically displayed when it is complete. To view the report again at a later time, go to the **My Reports** page to view the report in one of the two ways just described.



Figure 240. Viewing a Report

The selected report is displayed in the web client. Some types of report only have text ([Figure 240](#)), while others may include charts ([Figure 241](#)). Information included in the report is determined by the [Selection Criteria](#) that you set up when creating the report. The logo displayed at the top is defined on the [Customize](#) page.

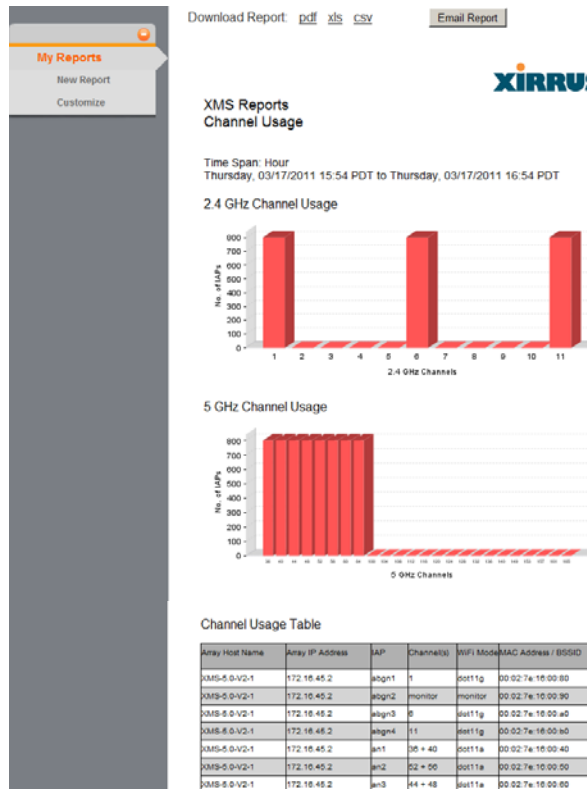


Figure 241. Report Including Charts

If the report had a time span setting, then the **Time Span** that you selected is shown underneath the title. It also identifies the data collection **Sample Period** used for the report. The sample period is automatically determined based on the Time Span. For long time spans, such as a year, the period will be longer (e.g., one

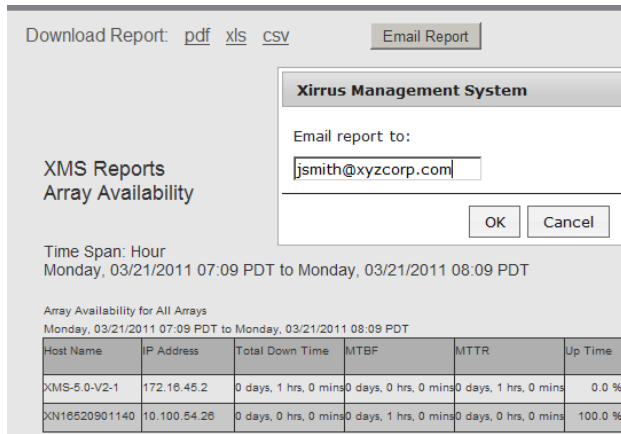
day). Short reporting periods, such as an hour, will be more granular and may have a period of 5 minutes.

The report may only be viewed as presented. You cannot sort columns or resize their width. Note that for very long reports, the HTML version is truncated to three pages so it will be able to be loaded in a browser. To view the full report, download it in PDF format as described below.

To download or view the report in a format other than HTML, select **pdf**, **xls**, or **csv** from the top of the page. The **File Download** dialog box will ask whether you wish to **Open** or **Save** the file. Select **Save** to specify where to save the file in your file system. Select **Open** to view the file using the appropriate software. By default, Acrobat is used to open PDFs and Excel is used for .csv and .xls files (unless you have changed the settings on your computer to open these files with a different application).

To print the report, we recommend that you download it as a PDF and print it from Acrobat.

To email the report, click the **Email Report** button at the top. (**Figure 242**) (Note that this button may not be displayed if you have not specified a mail server that XMS can use to send emails, as described in [“Web Client—Email Settings” on page 515.](#))



Download Report: [pdf](#) [xls](#) [csv](#) [Email Report](#)

Xirus Management System

Email report to:

**XMS Reports
Array Availability**

Time Span: Hour
Monday, 03/21/2011 07:09 PDT to Monday, 03/21/2011 08:09 PDT

Array Availability for All Arrays
Monday, 03/21/2011 07:09 PDT to Monday, 03/21/2011 08:09 PDT

Host Name	IP Address	Total Down Time	MTBF	MTTR	Up Time
XMS-5.0-V2-1	172.16.45.2	0 days, 1 hrs, 0 mins	0 days, 0 hrs, 0 mins	0 days, 1 hrs, 0 mins	0.0 %
XN16520901140	10.100.54.26	0 days, 0 hrs, 0 mins	0 days, 1 hrs, 0 mins	0 days, 0 hrs, 0 mins	100.0 %

Figure 242. Emailing a Report

The web client will prompt you to enter the email address, then click **OK**. A message will appear near the top of the page when the email has been successfully sent. The email displays the report in the same format shown on the web client page (i.e., HTML format), and there will be three attachments, one for each other format (PDF, .xls, .csv). Be aware that for large reports, the email size may be quite large.

New Report

To create a new report, click the **Reports** button at the top of the web client window, then click the **New Report** link.

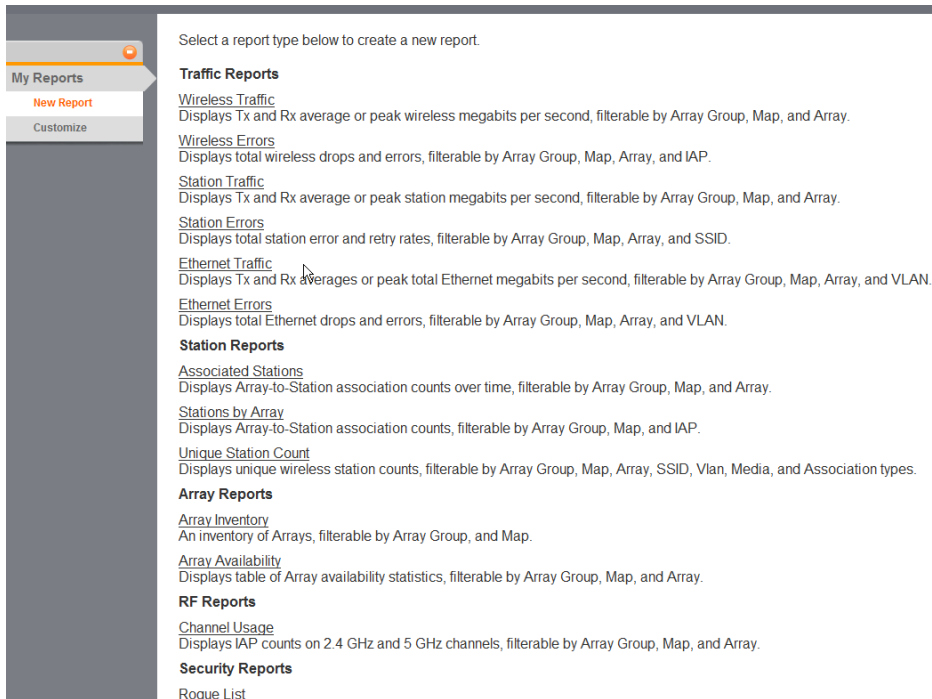


Figure 243. List of New Report Types

This page lists all of the report types offered by the web client. Click the desired report type, and the **Create New Report** page for the chosen report type is displayed. (Figure 244)

Create New Report

Type: Ethernet Errors

Displays total Ethernet drops and errors, filterable by Array Group, Array, and VLAN.

Name

Ethernet Errors - SS

Options

Group	All Arrays
Array	XMS-5.0-V2-1
VLAN	<div><div><div>VLAN Number</div><div>VLAN Name</div></div><div>All VLANs</div></div>
Table row limit	Show all
Date/Time	<div><div><div>Time Span</div><div>Last Hour</div></div><div><div>Specific Date Range</div><div>Date from:Time from:Date to:Time to:</div></div></div>

Schedule

Enable Schedule

Schedule Type:

Daily

Weekly

Monthly

Time of Day (24 hh:mm):05:57

Email Report To

Add

Save Report

Save & Run

Figure 244. Create New Report Page

The **Create New Report** page sets up the name and parameters for this report, especially the selection criteria use to filter the data included in the report. You may choose to run the report immediately after creating it, schedule it to run later at a specific time, or just save it without running it. Regardless, the report setup is always saved to the **My Reports** list, where you may run it or view previous results at any time. You may also choose to email the report after it runs.

The following topics are discussed for the New Reports page:

- **“Types of Reports” on page 380**
- **“To create a report” on page 381**
- **“Report Queue” on page 383**

Types of Reports

There are five categories of reports, listed below. Each report type may be filtered to select only the desired data. For example, you may select only certain Arrays or Array groups to include in the report. For details, see **“Selection Criteria” on page 384**. The available selection criteria vary for each report. They are listed in the detailed description of each report.

Traffic reports

These reports display wireless traffic and error statistics for radios, Ethernet ports, and stations.

- **Wireless Traffic**—Tx and Rx average or peak megabits per second. The wireless reports include all the data from the station reports (below) plus Wi-Fi management traffic such as beacons, probe requests, etc.
- **Wireless Errors**—total wireless drops and errors.
- **Station Traffic**—Tx and Rx average or peak megabits per second for traffic that flows to or from all associated stations.
- **Station Errors**—total station drops and errors.
- **Ethernet Traffic**—Tx and Rx averages or peak total megabits per second for the Array gigabit Ethernet ports.
- **Ethernet Errors**—total drops and errors for the Array gigabit Ethernet ports.

Station Reports

These reports display statistics related to station counts and Array-to-Station associations.

- **Associated Stations**—a list of stations associated to the Wi-Fi network.
- **Stations By Array**—Array-to-Station association counts.

- **Unique Station Count**—wireless station counts.

Array Reports

These reports display information about managed Arrays and their reliability statistics.

- **Array Inventory**—an inventory of Arrays.
- **Array Availability**—table of Array availability statistics.

RF Reports

This report displays information about channel usage.

- **Channel Usage**—IAP counts on 2.4 GHz and 5 GHz channels.

Security Reports

This report displays information about detected rogue APs.

- **Rogue List**—list of rogue access points detected by the Wi-Fi network.

To create a report

Enter the following information to set up the report.

- **Name**

This is a unique name that will identify this report on the **My Reports** page. You may create different reports of the same report type, with different options defined for each. Each report must have its own name. XMS will not allow you to create a new report using a name that is already in the My Reports list.
- **Options**

These settings define the selection criteria for the report. The types of criteria shown will differ by report type. They typically select criteria such as the Arrays and time period to be included in the report. For details on setting up these options for the report, please see **“Selection Criteria” on page 384**.

● Schedule

You may schedule the report to be automatically run on a recurring schedule. Click **Enable Schedule** to display time settings. Select one of the following options:

Hourly—Select the **minutes after the hour** when the report is to be run every hour. For example, to run the report on the hour, every hour, select **00**.

Daily—Enter the **Time of Day** when the report is to be run every day, based on a 24-hour time notation. For example, midnight is 00:00, half past noon is 12:30 and 4 PM is 16:00.

Weekly—Select the day of the week when the report is to be run, and then enter the **Time of Day** when the report is to be run, as described above.

Monthly—Select the day of the month when the report is to run, and then enter the **Time of Day** for the run, as described above.



You should use the Time Span option when scheduling reports, because the Specific Date Range option will just generate the same report over and over again.

● Email Report To

If you wish to have this report emailed to yourself or other recipients each time it runs, enter an email address and click the **Add** button. You may add multiple addresses. To remove an address from the email list, click the **X** in front of the entry. The email will display the report in the same format that is used to display it on the web client page (i.e., HTML format), and there will also be three attachments, one for each other format (PDF, .xls, .csv). Be aware that for large reports, the email size may be quite large.



You must specify the email server that XMS will use to send the email. Please see **“Web Client—Email Settings” on page 515**.

- Save Report / Save& Run

When the settings for the report are complete, click **Save Report** to simply add it to the **My Reports** list without running it. Click **Save & Run** to add it to the **My Reports** list and run it immediately. The **Report Queue** page will be displayed, showing the status of the report. You may navigate to another page while the report is being generated. Use the **My Reports** page to view the report later on.

Report Queue

When you run a new or saved report, or when the time comes to run a scheduled report, it is added to the Report Queue. Reports are run one at a time, in the order in which they are added to the queue. The queue displays the status of each report that is waiting to be run—**Pending** or **In progress**.

The report queue page is displayed only when you run a new or saved report immediately, but not when you schedule a report. On the report queue page, you may wait for an in progress report to complete, at which time the report will automatically be displayed. Or you may navigate away from the report queue page to perform other tasks with the web client. In this case, you may view the report later after it completes by using its entry on the **My Reports** page.

My Reports

New Report

Customize

Your report has been queued. This page will be redirected when the report is complete. Reports with a large amount of data can take a while to complete. If you do not want to wait, you can leave this page at any time and return to the Reports view later to view your report when it completes.

Report Queue:

Report	Status	Scheduled Time
Stations over Time SS	in progress <div style="display: inline-block; width: 100px; height: 10px; background: linear-gradient(to right, #0070c0 60%, #ccc 60%);"></div>	May 4, 2011 10:40:54 AM PDT

Figure 245. Report Queue

Selection Criteria

The web client presents you with a set of options for filtering (restricting) the data that it includes in a report. Different selection criteria are appropriate for different report types, thus the settings that you may specify are tailored for each type of report. This section will describe how to use selection criteria. The detailed description of each report type later in this chapter will list the selection criteria that are available for that report.

Open the **Create New Report Page** for the desired type of report as described in **“New Report” on page 378**. Choose your selection criteria in the **Options** section. You may select no options, or one or more options. Remember that each type of report will use its own subset of these settings. In all cases, you may select only one entry from each drop-down list.

When you choose values for a number of different selection criteria, the report will use only data that satisfies all of them—in other words, the report is based on the intersection of the conditions that you set. For example, if you select a **Group** and a **Radio**, the report will show results for just the selected radio on all Arrays in that group. Take some care so that you don’t choose criteria that will yield no results.

- **Group**—the drop-down list shows all of the Array Groups that you have defined in XMS. Array Groups are used as a convenient way to allow you to apply uniform configuration and handling to multiple Arrays at the same time. Select an Array group to report on just the Arrays that are members of the group, or select **All Arrays**. For more information, see **“Groups” on page 366**.
- **Map**—the drop-down list shows all of the maps that you have defined in XMS. Each map may have multiple Arrays located on it, and an Array may only belong to one map. Select a map to report on just the Arrays that are assigned to the map, or select **All Maps**. For more information, see **“Working with Maps” on page 129**.
- **Array**—the drop-down list shows all of the Arrays being managed in XMS. Select an Array to report on just that one Array, or select **All Arrays**. You cannot make more than one choice from the drop-down list.

- **Radio**—Select a radio (IAP) to report on just data for that one radio, or select **All Radios**. For more information, see [“IAPs” on page 309](#).
- **SSID**—the drop-down list shows all of the SSIDs that you have defined in XMS. Select an SSID to report on just data for that one SSID, or select **All SSIDs**. For more information, see [“VLAN” on page 259](#).
- **Media Type**—the drop-down list shows the IAP modes that are available on Arrays: **802.11b**, **802.11g**, **802.11a**, **802.11n**. Select a mode to report on just data for Array radios operating in that mode, or select **All Modes**.
- **Association**—select **Authenticated** from the drop-down list to show only stations that have been authenticated, or select **Any** to show all stations.
- **VLAN**—the drop-down list shows all of the VLANs that you have defined in XMS. You may choose to display them by **VLAN Number** or by **VLAN Name**. Select a VLAN to report on just data for that one VLAN, or select **All VLANs**. For more information, see [“VLAN” on page 259](#).
- **Classification**—the drop-down list allows you to select whether to report only on rogue IAPs whose classification matches your selection (select one of **Approved**, **Known**, **Unknown**, **Unclassified**, **Blocked**, or **Ad Hoc**) or select **All** to display rogues of any classification.
- **Detail on**—this setting specifies how you would like to break out report results. It is used by the [Unique Station Count](#) report. Select **Total** to show the total station count only, or you may break out detailed counts by **Array Name**, **VLAN Name**, **VLAN Number**, **SSID**, **Media Type**, **Radio**, or **Association Type**. The drop-down list allows you to select one of these parameters for detailing. For example, if you select detail on **VLAN**, the chart and the table will each will show one line for each VLAN.
- **Display traffic by**—the drop-down list allows you to select **Tx+Rx** to display transmit, receive, and total traffic broken out separately into three lines, or select **Total** to display only the totals. **Total** will show two lines: the average value of Tx+Rx, and the peak value of Tx+Rx.
- **Order table by**—the drop-down list allows you to select the column to use for sorting results: **Array Name** (the default), **MAC Address**, **IP Address**, **Map**, or **Serial Number**.

- **Order direction**—select **Ascending** or **Descending** sort order from the drop-down list.
- **Table row limit**—select the total number of rows to display in the report from the drop-down list: **10**, **20**, **50**, or **Show all**.
- **Date/Time**—this defines the time interval covered by the report, specified in terms of **Time Span** or **Specific Date Range**. In either case, the report will state the start time and end time of the period that it covers.

Select **Time Span** to specify a period ending at the report's run time. For example, if you select **Last Hour**, then the report will include data from the 60 minutes prior to the time when the report runs. You may select any entry in the drop-down list, for example **Last 24 Hours** or **Last 30 Days**. You should use the **Time Span** option when scheduling reports, because the **Specific Date Range** option will just generate the same report over and over again.

Select **Specific Date Range** to specify a start time and end time for the data to be included in the report. Click in the **Date From** field and then click the desired starting date using the drop-down calendar. Click in the **Time From** field and the **Choose Time** drop-down appears. Set the desired starting time by dragging the sliders for **Hour** and **Minute**. Set the **Date to** and **Time to** fields in the same way.

Customize

This page allows you to change the appearance of the report by modifying its header. Use this page to add your custom logo to the header.

To create a new report, click the **Reports** button at the top of the web client window, then click the **Customize** link. The **Customize Report Header** page appears. (Figure 246)

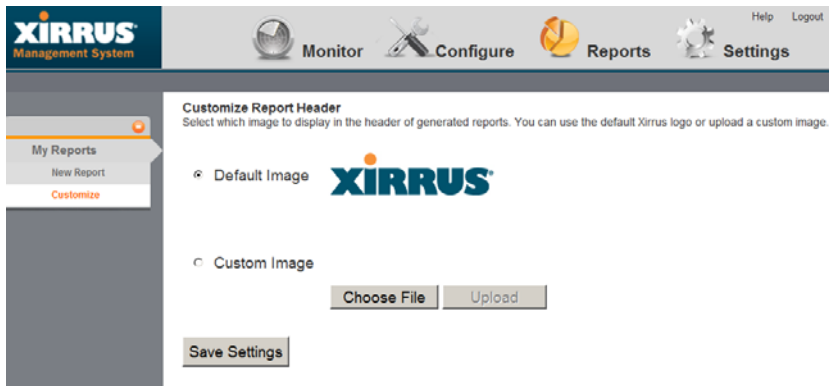


Figure 246. Customize Report Header Page

Select **Default Image** to use the default Xirrus logo at the top of all reports. Select **Custom Image** to upload your own logo to be used at the top of all reports. Click **Choose File** to browse to the desired image file. It must be one of the following types: .bmp, .jpg, .png. Then click the **Upload** button. Click **Save Settings** when done. Note that XMS does not impose a particular size limit on the image file, but the Xirrus logo is approximately 200 x 50 pixels, if you wish to use it as a guide.

The currently selected image will apply to all subsequent report runs (from either **New Reports** or **My Reports**). It will not affect any previously run reports—they will use the customization settings that were current at the time they were run.

Traffic Reports

Throughput is a measure of the amount of data that is transmitted in a given amount of time, expressed in bits per second (bps). Wi-Fi Arrays are designed to handle Gigabit Ethernet speeds, providing a throughput of 1000 Mbps (or 1 Gbps)—also known as 1000Base-T. One Gigabit is 10^9 bits per second, or 1,000,000,000 bps.

With their high-speed capability, your Wi-Fi Arrays can easily handle time-sensitive traffic, such as voice and video. The high capacity XN16 Wi-Fi Array has two Gigabit uplink ports and a total of 16 IAPs, providing a maximum wireless capacity of up to 4.8 Gbps, which offers ample reserves for the high demands of current and future applications.

The results returned for all reports in this section are dependent on the reporting period you specify. Throughput reports include:

- **Wireless Traffic**
Shows wireless throughput statistics for Arrays.
- **Wireless Errors**
Shows wireless error statistics for Arrays.
- **Station Traffic**
Tx and Rx average or peak megabits per second for traffic that flows to or from all associated stations.
- **Station Errors**
Provides wireless error statistics for stations.
- **Ethernet Traffic**
Shows Ethernet throughput statistics for Arrays.
- **Ethernet Errors**
Shows Ethernet error statistics for Arrays.

Wireless Traffic

This report provides statistical data for wireless throughput, based on the traffic flow achieved by each Wi-Fi Array. (Figure 247) The graph at the top of the window displays wireless data summed over the selected Arrays for the selected time range.

A table shows throughput for each Array, broken out by individual IAPs. The information displayed in this window and in the graph is dependent on the selection criteria you specify, summarized below.

Selection Criterion	Description (see “Selection Criteria” on page 384 for details)
Group	Include only Arrays that are members of the selected Array group.
Map	Include only Arrays that are members of the selected map.
Array	Include only the selected Array.
Display Traffic by	Break out transmit and receive traffic separately, or show only totals.
Table Row Limit	Total number of rows.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See “Schedule” on page 382.
Email Report To	After running, email the report . See “Email Report To” on page 382.

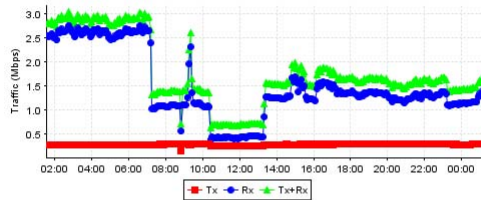
If you have a large network, the results returned in this report may span many pages. The browser display of the report will truncate to three pages to give you a preview—to see the entire report open the PDF version.



XMS Reports Wireless Traffic Tx+Rx

Time Span: Day
Wednesday, 04/13/2011 01:32 PDT to Thursday, 04/14/2011 01:32 PDT

Wireless Traffic Tx+Rx



Wireless Traffic Tx+Rx

Row Count: 13

Array Hostname	Array IP Address	AP Name	AP MAC Address	Min (Mbps)	Max (Mbps)	Avg (Mbps)
XN16520901140	10.100.54.26	abgn1	00:0f:7d:07:46:20-2e	0.000	0.000	0.000
XN16520901140	10.100.54.26	abgn2	00:0f:7d:07:46:60-6e	0.000	0.000	0.000
XN16520901140	10.100.54.26	abgn3	00:0f:7d:07:46:a0-ae	0.000	0.000	0.000
XN16520901140	10.100.54.26	abgn4	00:0f:7d:07:46:e0-es	0.000	0.000	0.000
XN16520901140	10.100.54.26	an1	00:0f:7d:07:46:10-1e	0.000	0.000	0.000
XN16520901140	10.100.54.26	an10	00:0f:7d:07:46:d0-de	0.000	0.000	0.000
XN16520901140	10.100.54.26	an11	00:0f:7d:07:46:f0-fe	0.000	0.000	0.000
XN16520901140	10.100.54.26	an12	00:0f:7d:07:46:00-0e	0.000	0.000	0.000
XN16520901140	10.100.54.26	an2	00:0f:7d:07:46:30-3e	0.000	2.635	1.130
XN16520901140	10.100.54.26	an3	00:0f:7d:07:46:40-4e	0.000	0.000	0.000
XN16520901140	10.100.54.26	an4	00:0f:7d:07:46:50-5e	0.000	0.000	0.000
XN16520901140	10.100.54.26	an5	00:0f:7d:07:46:70-7e	0.000	0.000	0.000
XN16520901140	10.100.54.26	an6	00:0f:7d:07:46:80-8e	0.000	0.000	0.000

Figure 247. Wireless Traffic Report

Table Details for the Wireless Traffic Report

The table portion of the report shows traffic statistics for each IAP on the selected Arrays, organized by the following column headers:

- **Array Hostname**

The host name assigned to the Array. Only Arrays that meet your selection criteria are included.

- **Array MAC Address**

This is the Array's MAC address.

- **IAP Name**
Each IAP in each Array is listed.
- **IAP MAC Address**
This is the IAP's MAC address.

Throughput data shown in the table depends on your **Selection Criteria**. If you set **Display Traffic by** to **Tx+Rx**, these columns are shown:

- **Min. (Mbps)**
Shows the minimum throughput (in megabits per second) achieved by the IAP for the time period you specified.
- **Max. (Mbps)**
Shows the maximum throughput (in megabits per second) achieved by the IAP for the time period you specified.
- **Avg. (Mbps)**
Shows the average throughput (in megabits per second) achieved by the IAP for the time period you specified.

If you set **Display Traffic by** to **Total**, these columns are shown:

- **Average Tx/Rx (Mbps)**
Shows the average total throughput (in megabits per second) achieved by the IAP for the time period you specified.
- **Peak Tx/Rx (Mbps)**
Shows the maximum total throughput (in megabits per second) achieved by the IAP for the time period you specified.

Wireless Errors

This report shows wireless communication error statistics for Array IAPs in the XMS managed network, based on your [Selection Criteria](#).

Selection Criterion	Description (see “Selection Criteria” on page 384 for details)
Group	Include only Arrays that are members of the selected Array group.
Map	Include only Arrays that are members of the selected map.
Array	Include only the selected Array.
Radio	Include only errors for the selected radio (IAP).
Date/Time	Include only this time range.
Schedule	Run the report at this time. See “Schedule” on page 382 .
Email Report To	After running, email the report . See “Email Report To” on page 382 .

Array errors reported are packet error rate, packet retry rate, and encryption retry rate, shown as a percentage of the total number of packets. ([Figure 248](#)) The graph shows the overall error percentages for all Arrays.

Table Details for the Wireless Errors Report

The results shown in this report are organized by the following column headers, which can be [sorted](#) to best suit your viewing needs:

- **Array Host Name**
The host name assigned to the Array.
- **Array MAC Address**
This is the Array’s MAC address.
- **Array IP Address**
The IP address assigned to the Array.

- **Packet Error Rate**

The packet error rate shown in this window reflects the bit errors detected by the system during the time period that you specified. The percentage shown is the number of bit errored packets divided by the total number of packets.

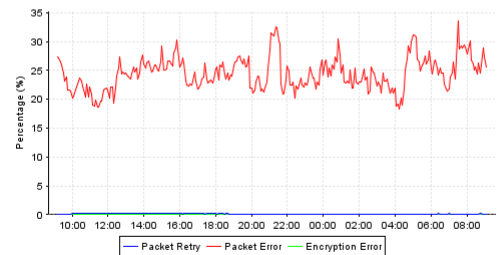
Download Report: [pdf](#) [xls](#) [csv](#) [Email Report](#)



XMS Reports
Wireless Errors

Time Span: Day
Sunday, 04/10/2011 09:08 PDT to Monday, 04/11/2011 09:08 PDT

Average Wireless Errors



Wireless Errors for Individual Array

Array Hostname	Array MAC Address	Array IP Address	Packet Error Rate	Packet Retry Rate	Encryption Error Rate
XN16520901140	00:0f:7d:00:91:7a	10.100.54.26	27.910 %	0.000 %	0.000 %

Figure 248. Wireless Errors Report

- **Packet Retry Rate**

Shows how many attempts were made to re-send dropped packets during the time period you specified. The percentage shown is the number of packet retries divided by the total number of packets.

- **Encryption Error Rate**

Shows how many attempts were made to reconcile security issues. The percentage shown is the number of received encryption errors divided by the total number of received packets.

Station Traffic

This report provides statistical data for throughput for the selected time period, based on the traffic flow achieved by each client station associated to the selected Arrays. (Figure 249) Throughput summed over all stations is represented in a graph at the top of the window. Throughput broken out by station is detailed in a table underneath.

The information displayed in this window is dependent on your **Selection Criteria**. There are two types of throughput data displayed, based on your choice for **Display Traffic by**:

- If you select **Tx+Rx**, both graph and table display average transmit, receive, and total traffic broken out separately into three lines. Transmit throughput is shown in red (**Tx**), receive throughput is shown in blue (**Rx**), and total throughput is shown in green (**Tx+Rx**).
- Select **Total** to display two lines: the average value of Tx+Rx in green, and the peak value of Tx+Rx in magenta.

Selection Criterion	Description (see “ Selection Criteria ” on page 384 for details)
Group	Include only Arrays that are members of the selected Array group.
Map	Include only member Arrays of the selected map.
Array	Include only the selected Array.
Display Traffic by	Break out transmit and receive traffic separately, or show only totals.
Table Row Limit	Total number of rows.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See “ Schedule ” on page 382.
Email Report To	After running, email the report . See “ Email Report To ” on page 382.

If you have a large network the results returned in this report may span many pages. The browser display of the report will truncate to three pages to give you a preview—to see the entire report open the PDF version.

Table Details for the Station Traffic Report

The results shown in this report are organized by the following column headers:

- **Array Hostname**
The host name of the Array to which the station is associated.
- **Station Hostname**
This column shows the host name for each client station listed in the report. The Station Hostname is specified for a device (in this case, a client station) when its networking is installed and configured. In order to connect to a computer running the TCP/IP protocol via its hostname (or Windows NetBIOS name), the name must be resolved to an IP address.

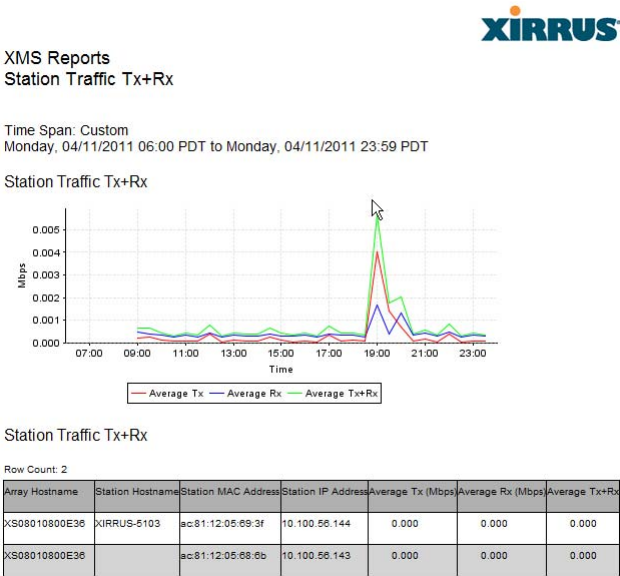


Figure 249. Station Traffic Report (Tx+Rx)

- **Station MAC Address**
This is the station's MAC address.
- **Station IP Address**
This is the station's IP address.

Throughput data shown in the table depends on your **Selection Criteria**. If you set **Display Traffic by** to **Tx+Rx**, these columns are shown:

- **Average Tx (Mbps)**
Shows the average transmit throughput (in megabits per second) achieved by the station for the time period you specified.
- **Average Rx (Mbps)**
Shows the average receive throughput (in megabits per second) achieved by the station for the time period you specified.
- **Average Tx+Rx (Mbps)**
Shows the average total throughput (in megabits per second) achieved by the station for the time period you specified.

If you set **Display Traffic by** to **Total**, these columns are shown:

- **Average Tx/Rx (Mbps)**
Shows the average total throughput (in megabits per second) achieved by the station for the time period you specified.
- **Peak Tx/Rx (Mbps)**
Shows the maximum total throughput (in megabits per second) achieved by the station for the time period you specified.

Station Errors

This report lists all stations with errors that were detected by XMS, based on your **Selection Criteria**.

Selection Criterion	Description (see “ Selection Criteria ” on page 384 for details)
Group	Include only Arrays that are members of the selected Array group.
Map	Include only Arrays that are members of the selected map.
Array	Include only the selected Array.
SSID	Include only the selected SSID.
Table Row Limit	Total number of rows.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See “ Schedule ” on page 382.
Email Report To	After running, email the report . See “ Email Report To ” on page 382.

Station errors reported in this window include the packet error rate and packet retry rate, where both categories are based on a percentage of the total number of these events detected by the system. **Figure 250** shows an example of the Error report for stations. The graph shows the packet error and packet dropped error percentages for all Arrays.

Table Details for the Station Errors Report

The results shown in this report are organized by the following column headers:

- **Array Hostname**
The host name of the Array that the station is associated with.
- **Station Hostname**
This column shows the host name of each client station in the report.

Station MAC Address

This is the station's MAC address.

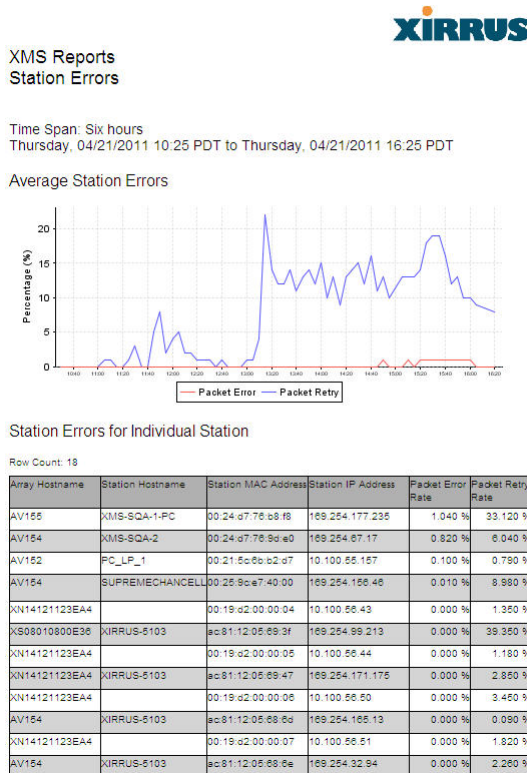


Figure 250. Station Errors Report

Station IP Address

The IP address assigned to the station.

Packet Error Rate%

The packet error rate shown in this window reflects the bit errors detected by the system during the time period you specified. The percentage shown is the number of packet errors divided by the total number of packets.

- **Packet Retry Rate%**

Shows how many attempts were made to re-send failed packets during the time period you specified. The percentage shown is the number of packet retries divided by the total number of packets.

Ethernet Traffic

This report provides statistical data for Ethernet throughput, based on the speeds achieved by the Gigabit1 Ethernet port on Wi-Fi Arrays. (**Figure 251**) The graph at the top of the window displays aggregate data throughput across all Arrays for the selected time range.

A table shows average and peak Ethernet rates for each Array. The information displayed in this window and in the graph is dependent on the selection criteria you specify, summarized below.

Selection Criterion	Description (see “ Selection Criteria ” on page 384 for details)
Group	Include only Arrays that are members of the selected Array group.
Map	Include only Arrays that are members of the selected map.
Array	Include only the selected Array.
VLAN	Include only the selected VLAN (specified by name or number)
Display Traffic by	Break out transmit and receive traffic separately, or show only totals.
Table Row Limit	Total number of rows.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See “ Schedule ” on page 382.
Email Report To	After running, email the report . See “ Email Report To ” on page 382.

If you have a large network, the results returned in this report may span many pages. The browser display of the report will truncate to three pages to give you a preview—to see the entire report open the PDF version.

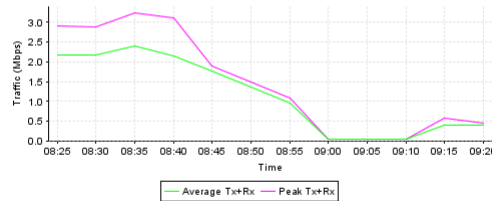
Download Report: [pdf](#) [xls](#) [csv](#) [Email Report](#)



XMS Reports Ethernet Traffic Total

Time Span: Hour
Monday, 04/11/2011 08:21 PDT to Monday, 04/11/2011 09:21 PDT

Ethernet Traffic Total



Ethernet Traffic Total

Array Hostname	Array MAC Address	Array IP Address	Average Tx/Rx (Mbps)	Peak Tx/Rx (Mbps)
XS08010800E36	00:0f:7d:00:5e:f2	10.0.11.1	0.237	0.299
XN16520901140	00:0f:7d:00:91:7a	10.100.54.26	0.048	0.052

Figure 251. Ethernet Traffic Report

Table Details for the Ethernet Traffic Report

The table portion of the report shows traffic statistics for the Gigabit1 port on selected Arrays, organized by the following column headers:

- Array Hostname**
The host name assigned to the Array. Only Arrays that meet your selection criteria are included.
- Array MAC Address**
This is the Array's MAC address.
- Array IP Address**
This is the Array's IP address.

Throughput data shown in the table depends on your **Selection Criteria**. If you set **Display Traffic by** to **Tx+Rx**, these columns are shown:

- **Average Tx (Mbps)**
Shows the average transmit throughput (in megabits per second) achieved by the Array for the time period you specified.
- **Average Rx (Mbps)**
Shows the average receive throughput (in megabits per second) achieved by the Array for the time period you specified.
- **Average Tx+Rx (Mbps)**
Shows the average total throughput (in megabits per second) achieved by the Array for the time period you specified.

If you set **Display Traffic by** to **Total**, these columns are shown:

- **Average Tx/Rx (Mbps)**
Shows the average total throughput (in megabits per second) achieved by the Array for the time period you specified.
- **Peak Tx/Rx (Mbps)**
Shows the maximum total throughput (in megabits per second) achieved by the Array for the time period you specified.

Ethernet Errors

This report shows Ethernet communication errors for the Gigabit ports in all Arrays in the XMS managed network, based on your **Selection Criteria**.

Selection Criterion	Description (see “ Selection Criteria ” on page 384 for details)
Group	Include only Arrays that are members of the selected Array group.
Map	Include only Arrays that are members of the selected map.
Array	Include only the selected Array.
VLAN	Include only the selected VLAN (specified by name or number)
Table Row Limit	Total number of rows.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See “ Schedule ” on page 382.
Email Report To	After running, email the report . See “ Email Report To ” on page 382.

Ethernet errors reported include packet error rate and packet retry rate, where both categories are based on a percentage of the total number of packets. (Figure 252)

Table Details for the Ethernet Errors Report

The results shown in this report are organized by the following column headers:

- **Array Hostname**
The host name assigned to the Array.
- **Array MAC Address**
This is the Array’s MAC address.

- **Array IP Address**
The IP address assigned to the Array.
- **Array Packets Error Rate**
The packet error rate reflects the bit errors detected by the system during the time period you specified. The percentage shown is the number of bit errors divided by the total number of packets.

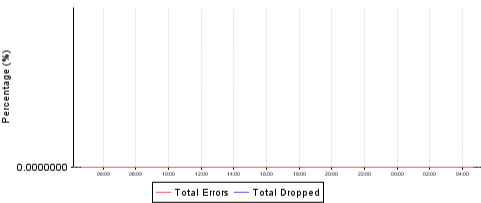
Download Report: [pdf](#) [xls](#) [csv](#) [Email Report](#)



XMS Reports
Ethernet Errors

Time Span: Day
Monday, 04/11/2011 04:38 PDT to Tuesday, 04/12/2011 04:38 PDT

Average Ethernet Errors



Ethernet Errors for Individual Array

Array Hostname	Array MAC Address	Array IP Address	Array Packets Error Rate	Array Packets Drop Rate
XN16520801140	00:0f:7d:00:91:7a	10.100.54.26	0.000 %	0.000 %
XS08010800E36	00:0f:7d:00:5a:f2	10.0.11.1	0.000 %	0.000 %

Figure 252. Ethernet Errors Report

- **Array Packets Drop Rate**
Shows how many packets failed due to being dropped during the time period you specified. The percentage shown is the number of packets dropped divided by the total number of packets.

Station Reports

A basic wireless network consists of an Access Point (AP) and client stations that are associated to the network via the AP. Each Wi-Fi Array includes a number of IAPs (Integrated Access Points), with each IAP capable of associating up to 96 client stations. The high capacity XN16 Wi-Fi Array has 16 IAPs, which means the Array can associate up to 1536 stations (16 x 96). And because XMS can support many Arrays, the number of clients that can be associated may be quite large. Note that typically, the **abg2/abgn2** IAP is enabled for monitoring only (default), and client stations cannot associate with this IAP.

The following reports are available in this section:

- **Associated Stations**
Provides station association data for the selected Arrays.
- **Stations By Array**
Allows you to review station association data based on selected Arrays, including how many stations were associated at the busiest (peak) time.
- **Unique Station Count**
This report displays a line graph showing station counts over time, broken out into categories by your choice of categories such as SSID and VLAN.

Associated Stations

This report consists of a table listing stations that are associated to your Wi-Fi network. (Figure 253) The information displayed in this window is based on your **Selection Criteria**. You may use the criteria to report on just those stations that are associated to the selected Arrays.

Selection Criterion	Description (see “Selection Criteria” on page 384 for details)
Group	Include only Arrays that are members of the selected Array group.
Map	Include only Arrays that are members of the selected map.
Array	Include only the selected Array.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See “Schedule” on page 382.
Email Report To	After running, email the report . See “Email Report To” on page 382.

Discrete Array to Station Association

This table presents a list of all stations associated to the selected Arrays based on the time period you specify. The results shown in this window are organized by the following column headers:

- **Array Host Name**
The host name of the Array that the station is associated with.
- **Array MAC Address**
The MAC address of the Array that the station is associated with.
- **Station Hostname**
This column shows the name for each client station listed in the report.
- **Station MAC Address**
This is the station’s MAC address.

Station IP Address

The IP address assigned to the station.

Download Report: [pdf](#) [xls](#) [csv](#) [Email Report](#)



XMS Reports
Station Association

Time Span: Hour: Period: 5 Minutes
Wednesday, 05/04/2011 09:10 PDT to Wednesday, 05/04/2011 10:10 PDT
(Report generated on 05/04/2011 at 10:40:59 PDT.)

Discrete Array to Station Association

Row Count: 9

Array Hostname	Array MAC Address	Station Hostname	Station MAC Address	Station IP Address
Location-Lobby	00:0f:7d:00:d2:a2	(empty)	7c:d5:37:3b:36:f6	10.100.46.111
Location-Lobby	00:0f:7d:00:d2:a2	(empty)	5c:59:48:29:48:4f	10.100.46.114
Location-Lobby	00:0f:7d:00:d2:a2	DMOXLEY-0910P	00:21:5c:23:13:85	10.100.46.119
Location-Support	00:0f:7d:00:76:48	XIRRUS-5103	ac:81:12:05:69:6d	10.100.46.110
Location-Support	00:0f:7d:00:76:48	(empty)	a4:67:06:b7:35:e8	10.100.46.112
XS08010800E38	00:0f:7d:00:5e:f2	XIRRUS-5103	ac:81:12:05:69:3f	10.100.56.144
XS08010800E38	00:0f:7d:00:5e:f2	XIRRUS-5103	ac:81:12:05:69:6b	10.100.56.143
XS391906003AE	00:0f:7d:00:43:66	(empty)	00:19:d2:1b:5f:f4	(empty)
XS_39-10.100.40.37	00:0f:7d:00:42:9b	(empty)	00:19:d2:05:8a:64	(empty)

Figure 253. Station Association

Stations By Array

This report displays a bar chart showing the number of stations associated to those Arrays that have the highest station count. (Figure 254) The information displayed in this window is based on your [Selection Criteria](#).

Selection Criterion	Description (see "Selection Criteria" on page 384 for details)
Group	Include only Arrays that are members of the selected Array group.
Map	Include only Arrays that are members of the selected map.
Radio	Include only errors for the selected radio (IAP).

Selection Criterion	Description (see “ Selection Criteria ” on page 384 for details)
Date/Time	Include only this time range.
Schedule	Run the report at this time. See “ Schedule ” on page 382.
Email Report To	After running, email the report . See “ Email Report To ” on page 382.

Total Array to Station Associations

This table shows the minimum and maximum number of stations that have been associated to each Array, with the following information:

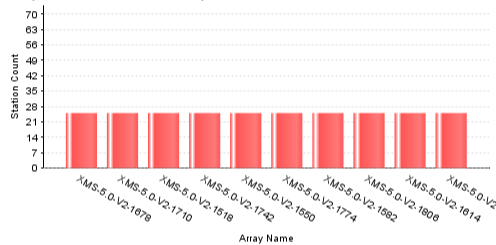
- **Array Name**
The host name assigned to the Array.
- **Array MAC Address**
This is the Array’s MAC address.
- **Array IP Address**
The IP address assigned to the Array.
- **Minimum Simultaneous**
Shows the lowest number of stations concurrently associated to each Array during the time period.
- **Maximum Simultaneous Stations**
Shows the number of stations that were concurrently associated to each Array at the busiest (peak) time during the time period.
- **Unique Stations**
Shows the total number of different stations that have associated to each Array over the time period.

Download Report: [pdf](#) [xls](#) [csv](#)
[Email Report](#)


XMS Reports Stations By Array

Time Span: Hour
Tuesday, 03/22/2011 07:34 PDT to Tuesday, 03/22/2011 08:34 PDT

Top Arrays for Station Count for All Arrays
Tuesday, 03/22/2011 07:34 PDT to Tuesday, 03/22/2011 08:34 PDT



Total Array to Station Associations

Array Name	Array MAC Address	Array IP Address	Minimum Simultaneous	Maximum Simultaneous	Unique Stations
XMS-5.0-V2-1	00:02:7e:16:00:52	172.16.45.2	25	25	25
XMS-5.0-V2-1001	00:02:7e:20:00:52	172.16.49.2	25	25	25
XMS-5.0-V2-1501	00:02:7e:22:00:52	172.16.51.2	25	25	25
XMS-5.0-V2-1002	00:03:7e:20:00:52	172.16.49.3	25	25	25
XMS-5.0-V2-1502	00:03:7e:22:00:52	172.16.51.3	25	25	25
XMS-5.0-V2-1003	00:04:7e:20:00:52	172.16.49.4	25	25	25
XMS-5.0-V2-1503	00:04:7e:22:00:52	172.16.51.4	25	25	25
XMS-5.0-V2-4	00:05:7e:16:00:52	172.16.45.5	25	25	25
XMS-5.0-V2-1004	00:05:7e:20:00:52	172.16.49.5	25	25	25
XMS-5.0-V2-1504	00:05:7e:22:00:52	172.16.51.5	25	25	25
XMS-5.0-V2-5	00:06:7e:16:00:52	172.16.45.6	25	25	25
XMS-5.0-V2-1005	00:06:7e:20:00:52	172.16.49.6	25	25	25

Figure 254. Station Association (By Array) Report

Unique Station Count

This report displays a line graph showing unique station counts over time. “Unique” means that if the same station disconnects and then reconnects, it will not be counted more than once in any sum displayed.

The information displayed in this window is based on your **Selection Criteria**.

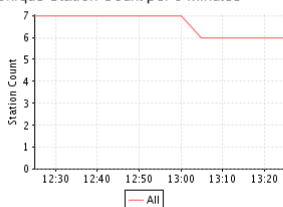
Selection Criterion	Description (see “ Selection Criteria ” on page 384 for details)
Group	Include only member Arrays of the selected Array group.
Map	Include only Arrays that are members of the selected map.
Array	Include only the selected Array.
SSID	Include only the selected SSID.
VLAN	Include only the selected VLAN (specified by name or number)
Media Type	Include only IAPs operating in the selected mode (802.11b, 802.11g, 802.11a, or 802.11n)
Association	Include only stations that are authenticated, or all stations.
Detail on	Break out counts by the selected category, or show only totals.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See “ Schedule ” on page 382.
Email Report To	After running, email the report . See “ Email Report To ” on page 382.

Download Report: [pdf](#) [xls](#) [csv](#)
[Email Report](#)


XMS Reports Unique Station Count

Time Span: Hour. Period: 5 Minutes.
Wednesday, 05/04/2011 12:25 PDT to Wednesday, 05/04/2011 13:25 PDT
(Report generated on 05/04/2011 at 13:58:09 PDT.)

Unique Station Count per 5 Minutes



Unique Stations this Period	
7	
Station Associations	
Lowest	Peak
6	7

Top Station Counts with Detail on Total

Row Count: 5

Array	Unique Stations Count
Location-Support	2
XS08010800E36	2
XS_39-10.100.40.37	1
Location-Lobby	1
XS391906003AE	1

Figure 255. Unique Station Count Report

The graph is detailed on (i.e., broken out into categories by) your choice of category:

- Total—show totals only.
- Array Name—show station count by Array.
- VLAN (by name or number)—show station count by VLAN.
- SSID—show station count by SSID.
- Media Type—show station count by radio mode: 802.11n, 802.11a, etc.
- Radio—show station count by IAP: an1, abgn1, etc.
- Association Type—show station count according to whether the connection is authenticated.

The graph has a separate line for each member of the detailing category. For example, if you detail on Radio as shown in [Figure 255](#), then there will be a separate line graph for each IAP: an1, an2, and so on. This report also shows you how many stations are currently online, and includes minimum (Lowest) and maximum (Peak) activity. A table at the bottom lists peak station counts broken out by your requested category.

Table Details for the Station Count Report

The table below the graph simply shows the peak station count for each member of the **Detail on** category.

Array Reports

Array status reports provide utility functions, such as listing all Arrays for you and showing reliability statistics.

The following reports are available in this section:

- **Array Inventory**
Provides a list of all Arrays in your managed Wi-Fi network, including serial numbers.
- **Array Availability**
This report shows reliability statistics for your managed Wi-Fi network, including MTBF and MTTR figures.

Array Inventory

This report creates an inventory list for your use. (Figure 256) The result is a list of all your managed Wi-Fi Arrays for your reference. You may find it very useful to save this report as a .csv or .xls file as a starting point for working with Excel. The report is based on your **Selection Criteria**.

Selection Criterion	Description (see “ Selection Criteria ” on page 384 for details)
Group	Include only Arrays that are members of the selected Array group.
Map	Include only Arrays that are members of the selected map.
Order table by	Sort table by selected column.
Order Direction	Sort in ascending or descending order.
Schedule	Run the report at this time. See “ Schedule ” on page 382.
Email Report To	After running, email the report . See “ Email Report To ” on page 382.

Table Details for the Array Inventory Report

The table portion of the report shows the name, addresses, and serial number of the selected Arrays, organized by the following column headers:

- **Array Name**
The host name assigned to the Array. Only Arrays that meet your selection criteria are included.
- **MAC Address**
This is the Array's MAC address.
- **IP Address**
This is the Array's IP address.
- **Location**
The physical location information that you entered for this Array, if any.
- **Serial Number**
This is the Array's serial number.

Download Report: [pdf](#) [xls](#) [csv](#) |

[Email Report](#)



XMS Reports
Array Inventory

Array Inventory

Wednesday, 03/16/2011 09:07:25 PDT

Array Name	MAC Address	IP Address	Location	Serial Number
XMS-5.0-V2-1900	01:92:7e:23:00:52	172.16.52.151		KN0824081A2E2
XMS-5.0-V2-1899	01:91:7e:23:00:52	172.16.52.150		KN0824081A2E2
XMS-5.0-V2-1898	01:90:7e:23:00:52	172.16.52.149		KN0824081A2E2
XMS-5.0-V2-1897	01:8f:7e:23:00:52	172.16.52.148		KN0824081A2E2
XMS-5.0-V2-1896	01:8e:7e:23:00:52	172.16.52.147		KN0824081A2E2
XMS-5.0-V2-1895	01:8d:7e:23:00:52	172.16.52.146		KN0824081A2E2
XMS-5.0-V2-1894	01:8c:7e:23:00:52	172.16.52.145		KN0824081A2E2
XMS-5.0-V2-1893	01:8b:7e:23:00:52	172.16.52.144		KN0824081A2E2
XMS-5.0-V2-1892	01:8a:7e:23:00:52	172.16.52.143		KN0824081A2E2
XMS-5.0-V2-1891	01:89:7e:23:00:52	172.16.52.142		KN0824081A2E2

Figure 256. Array Inventory Report

Array Availability

This report shows system reliability statistics for your Wi-Fi network, based on your **Selection Criteria**. **Figure 257** shows an example of the Array Availability report.

Selection Criterion	Description (see “Selection Criteria” on page 384 for details)
Group	Include only Arrays that are members of the selected Array group.
Map	Include only Arrays that are members of the selected map.
Array	Include only the selected Array.
Table Row Limit	Total number of rows.
Date/Time	Include only this time range.
Schedule	Run the report at this time. See “Schedule” on page 382.
Email Report To	After running, email the report . See “Email Report To” on page 382.

Download Report: [pdf](#) [xls](#) [csv](#) [Email Report](#)



XMS Reports Array Availability

Time Span: Day
Sunday, 04/10/2011 17:32 PDT to Monday, 04/11/2011 17:32 PDT

Array Availability for All Arrays
Sunday, 04/10/2011 17:32 PDT to Monday, 04/11/2011 17:32 PDT

Hostname	IP Address	Total Down Time	MTBF	MTTR	Up Time
XN10520901140	10.100.54.26	0 days, 0 hrs, 4 mins	0 days, 11 hrs, 57 mins	0 days, 0 hrs, 2 mins	99.7 %
XS08010800E36	10.100.56.31	0 days, 0 hrs, 0 mins	1 days, 0 hrs, 0 mins	0 days, 0 hrs, 0 mins	100.0 %

Figure 257. Array Availability Report

Table Details for the Array Availability Report

The Array Availability report is generated as a table. The results are organized by the following column headers:

- **Host Name**
The host name assigned to the Array.
- **IP Address**
The IP address assigned to the Array.
- **Total Down Time**
Shows the total time (in minutes) that this Array has been down within the time range specified for this report.
- **MTBF** (Mean Time Between Failures)
Shows the average length of time that elapsed between failures of the Array within the time range specified for this report—shown in days/hours/minutes.
- **MTTR** (Mean Time To Repair)
Shows the average length of time that elapsed before functionality to the Array was restored following a failure within the time range specified for this report—shown in days/hours/minutes.
- **Up Time%**
This is the time that the Array has been up and running successfully, based on a percentage of the total time for the time period specified for this report.



If XMS is non-operational for a period of time, Array availability information for this report is extrapolated from the last known state of the Array prior to XMS going off-line.

RF Reports

RF reports provide information on RF (channel) usage in your network. For more information about assigning channels, see [“IAPs” on page 309](#).

The following RF report is available:

- **Channel Usage**
Shows which channels each IAP is using.

Channel Usage

This report generates a table of current channel assignments for each IAP and for all media types (2.4 and 5 GHz channels), based on your [Selection Criteria](#).

Selection Criterion	Description (see “Selection Criteria” on page 384 for details)
Group	Include only Arrays that are members of the selected Array group.
Map	Include only Arrays that are members of the selected map.
Array	Include only the selected Array.
Table Row Limit	Total number of rows.
Schedule	Run the report at this time. See “Schedule” on page 382 .
Email Report To	After running, email the report . See “Email Report To” on page 382 .

The Channel Usage report also provides separate bar charts for the 2.4 GHz and 5 GHz bands, showing the number of IAPs using each channel. ([Figure 258](#))

Table Details for the Channel Usage Report

The results shown in this report are organized by the following column headers:

- **Array Hostname**
The host name assigned to the Array that the IAP belongs to.

- **Array IP Address**
The IP address assigned to the host Array.
- **IAP**
The name of the access point (for example, abg4, an3, a7, etc.). The **abg2/abgn2** IAP is usually enabled for monitoring only (default), which means that client stations typically cannot associate with this IAP.
- **Channel(s)**
This column shows the channel(s) used by the IAP. IEEE 802.11n radios use two adjacent bonded channels for improved performance, so those IAPs will show two channels if they have bonding in operation.



Figure 258. Channel Usage Report

- **Wi-Fi Mode**

This shows the IEEE 802.11 media in use by the IAP.

- **MAC Address / BSSID**

This is the IAP's MAC address.

Security Reports

The level of security you introduce into your network depends on the requirements of your deployment, though we strongly recommend that you do not configure your Arrays as Open Systems (no authentication required and no data encryption). An Access Control List (ACL) and/or WEP (Wired Equivalent Privacy) should be your minimum requirement for security. WPA and WPA2 offer even stronger security. The Wi-Fi Array's line rate encryption ensures high performance when encryption is in use. For more information about security, go to **"Security" on page 270**.

Security reports provide data based on the security parameters defined for your network of Arrays, including authentication and data encryption. The following security report is available:

- **Rogue List**

Shows all rogue APs that are visible on your network and provides charts that distinguish between **Unclassified**, **Approved**, **Known** or **Unknown** rogue devices.

Rogue List

A rogue is any wireless device that is visible on your network but not recognized as being an integral part of the network. Rogue detection is performed automatically and constantly by the built-in threat-sensor radio **abg2/abgn2** in each Array. XMS collects this information from the Arrays in its managed network. As access points are switched off and on, the list of detected rogues changes. Please see **“Security - Managing Intrusions” on page 119** for more information about rogues and their classifications and handling.

This report displays a color-coded pie chart representation of all rogue devices that have been detected by the portions of your network that you selected.

Selection Criterion	Description (see “Selection Criteria” on page 384 for details)
Group	Include only Arrays that are members of the selected Array group.
Map	Include only Arrays that are members of the selected map.
Array	Include only the selected Array.
SSID	Include only the selected SSID.
Classification	Include only rogue IAPs whose classification is Approved, Known, Unknown, Unclassified, Blocked, or Ad Hoc .
Schedule	Run the report at this time. See “Schedule” on page 382 .
Email Report To	After running, email the report . See “Email Report To” on page 382 .

The chart (**Figure 259**) shows the percentages of rogue devices based on their classifications.

- **Unclassified**
These rogues have not yet been classified.

- **Approved**
When a rogue is designated as Approved the system stops reporting on it and no longer displays it in the rogue list.

Download Report: [pdf](#) [xls](#) [csv](#) [Email Report](#)

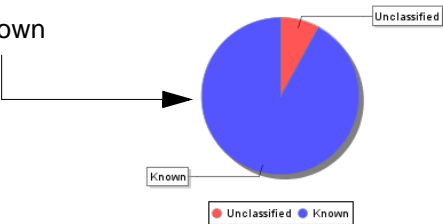


XMS Reports
Rogue List
- Array "XMS-5.0-V2-1"

Time Span: Hour
Monday, 03/28/2011 17:30 PDT to Monday, 03/28/2011 18:30 PDT

Rogue Classification

Approved/Known
/Unknown



All Classification

BSSID Vendor ID SSID	Detecting Array IP Address	Security	Channel	RSSI	Discovered	Last Active
00:0e:83:bf:db:7a -Cisco -ptest	XMS-5.0-V2-1 -172.16.45.2	TKIP+PSK	52	-69	null	
00:0f:24:08:e5:80 -Cisco -ptest	XMS-5.0-V2-1 -172.16.45.2	TKIP+PSK	6	-83	null	
00:0f:7d:00:89:a0 -Xirus -L3R-Open	XMS-5.0-V2-1 -172.16.45.2	none	6	-69	null	

Figure 259. Rogue List Report

- **Known**
When a rogue is designated as Known the system stops reporting on this rogue, but still displays it in the rogue list.
- **Unknown**
These rogues are always displayed in the rogue list.

- **Blocked**

These rogues have been designated as blocked. An Array can block this AP by preventing stations from staying associated to the rogue.

Table Details for the Security Report (Rogue List)

Below the pie chart is a table identifying all of the rogues included in the pie chart. The results shown in this table are organized by the following column headers:

- **BSSID—Vendor ID—SSID**

This shows the BSSID of the rogue device (typically its MAC address), the name of the equipment manufacturer of the rogue, and the SSID (network name) being broadcast by the rogue device. If the rogue has its SSID set to default and is configured to broadcast its SSID, then the entry in this field will be **default**. If the rogue is configured not to broadcast its SSID, then the entry in this field will be **(empty)**.

- **Detecting Array—IP Address**

Shows the host name and IP address of the Array that is detecting the rogue device.

- **Security**

Shows the [authentication](#) and [encryption](#) security levels detected on the rogue device (for example, AES+TKIP+EAP). If the rogue is running an open system—no security—the entry in this field is **none**.

- **Channel**

This is the channel that the rogue is detected on.

- **RSSI (Received Signal Strength Indicator)**

Shows the strength of the signal being observed from the rogue device by the detecting Array.

- **Discovered**

This is the date and time that the rogue was discovered by the detecting Array.

- **Last Active**

This is the date and time that the rogue was last seen by the detecting Array, or **Active** if the rogue is still active.

The XMS Web Client

The Web Client provides a fast, efficient interface for checking Wi-Fi network performance and for selected management tasks. This provides an alternative to using the Java Client for many management functions.

XMS also provides a Java Client interface, which offers a complete set of functions for monitoring and managing your Wi-Fi network. The current chapter discusses usage of the XMS web client. For more information about using the XMS Java client, please see the chapter titled **“The XMS Java Client Interface” on page 39**.

Starting the Web Client

The XMS web client requires one of the following browsers: Internet Explorer (version 7.0 or higher), Mozilla Firefox (version 3.0 or higher), Chrome (version 3.0 or higher), or Safari (version 5.0 or higher). A secure Web browser is required for the web client.

To start the web client, point your workstation’s browser to the IP address or hostname for the XMS server machine followed by :9090. For example, if the IP address is 192.168.10.40, point your browser to **http://192.168.10.40:9090**.

When the XMS splash window appears, click **Web Client**. (Figure 260)



Figure 260. XMS Start Window

Web Client Modes

The web client has different modes of operation, selected by buttons at the top of the window. Each mode offers a selection of pages which manage different XMS functions. The modes are described in the following sections:

- “About Monitor Pages” on page 424
- “About Configure Pages” on page 425
- “About Reports Pages” on page 427
- “About Settings Pages” on page 428

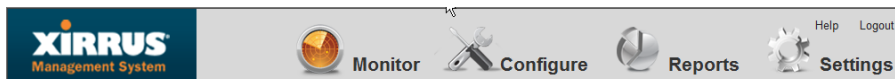


Figure 261. Mode Selection in XMS Web Client

About Monitor Pages

These pages display information about the current status of the network. Click the **Monitor** button at the top of the window to see the list of monitor pages on the left. These are primarily read-only pages, although most of the pages (except for the Dashboard) allow you to export data to a file. The Monitor button always opens to the Dashboard page.

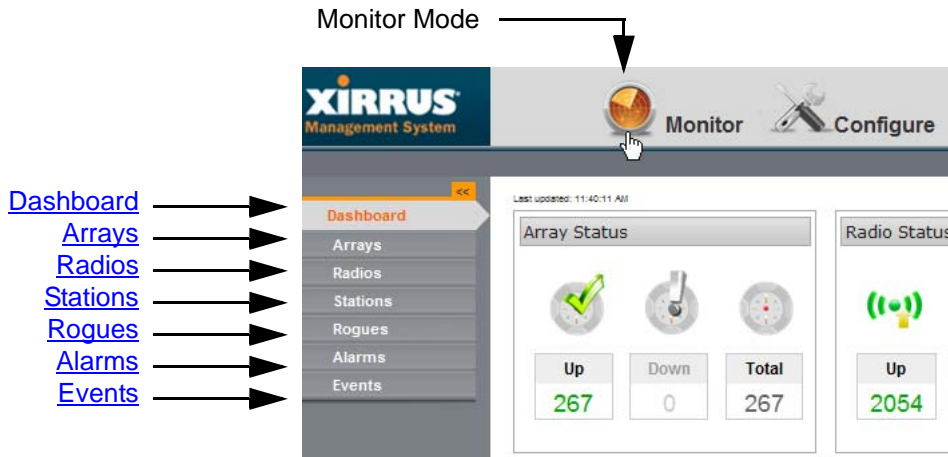


Figure 262. XMS Web Client Monitor Functions

Monitor pages include the following. Click one of the links below or in **Figure 262** for more information.


- **Dashboard**
- **Arrays**
- **Radios**
- **Stations**
- **Rogues**
- **Alarms**
- **Events**

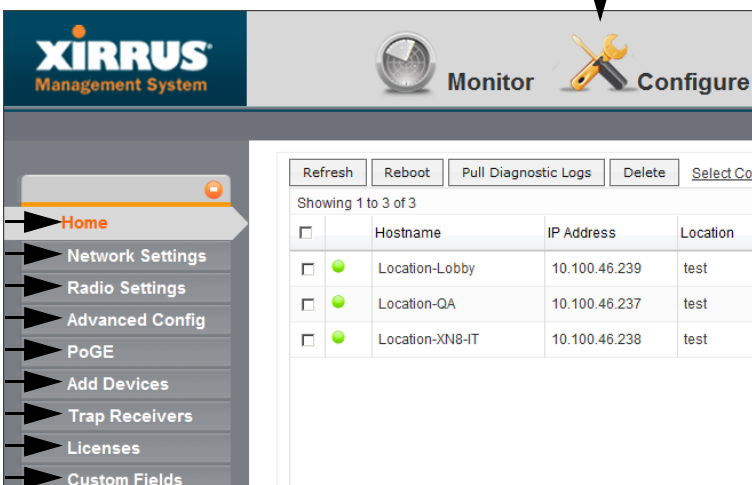
About Configure Pages


These pages perform specific Wi-Fi network configuration actions. Some of these pages are particularly powerful, allowing you to make bulk configuration changes over multiple radios and Arrays in one step. Click the **Configure** button at the top of the window to see the list of configure pages on the left. (**Figure 263**) The Configure button always opens to the Home page, which is the same as the **Arrays** page.


Configure pages include:


- **Configure—Home Page**
- **Network Settings**
- **Radio Settings**
- **Advanced Config**
- **PoGE**
- **Add Devices**
- **Trap Receivers**
- **Array Licenses**
- **Custom Fields**


Configure Mode 





Home  **Home**


[Network Settings](#)  Network Settings


[Radio Settings](#)  Radio Settings


[Advanced Config](#)  Advanced Config

[PoGE](#)  PoGE

[Add Devices](#)  Add Devices

[Trap Receivers](#)  Trap Receivers

[Array Licenses](#)  Licenses

[Custom Fields](#)  Custom Fields

	Hostname	IP Address	Location
<input type="checkbox"/>	Location-Lobby	10.100.46.239	test
<input type="checkbox"/>	Location-QA	10.100.46.237	test
<input type="checkbox"/>	Location-XN8-IT	10.100.46.238	test

Figure 263. XMS Web Client Configure Functions

About Reports Pages

These pages are used to generate reports on the operation of your Wi-Fi network. XMS offers an extensive suite of reports on performance and status, including such aspects as throughput, error rates, station information, availability, RF usage, and security.

All of these reports are discussed in detail in **“Managing Reports” on page 371**.

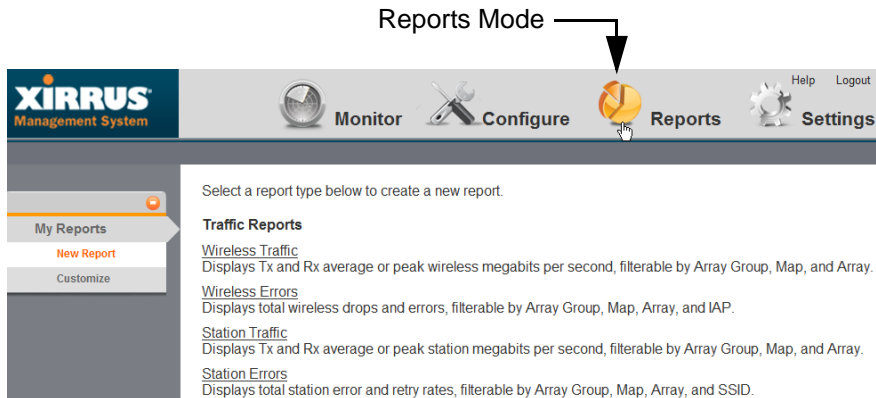


Figure 264. XMS Web Client Reports Functions

Click the **Reports** button at the top of the window to see the list of reports pages on the left.

- **“My Reports” on page 373**

The web client’s **Reports** button opens to this page, listing the reports you have already created and allowing you to view or run these reports.

- **“New Report” on page 378**

This page lists all the types of reports available in XMS. Click on a report, and enter the desired selection criteria. You may then save the report and run it now or schedule it for later.

- **“Customize” on page 387**

Click this link to customize the appearance of reports by changing the logo at the top of the report.

About Settings Pages

These pages are used to change XMS server settings, such as polling rate and backup schedules. In addition, if you are using a Linux-based Xirrus Management Appliance (see [“About the XM-3320, XM-3340, and XM-3360” on page 14](#)), use these pages to configure the appliance, including setting the network address and system date and time. All of these server administration functions are discussed in detail in [“About Managing the XMS Server” on page 501](#).

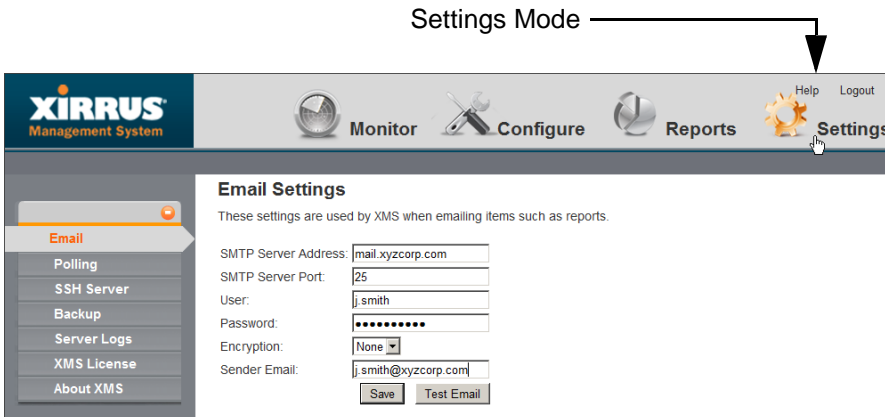


Figure 265. XMS Web Client Settings Functions

Click the **Settings** button at the top of the window to see the list of settings pages on the left.

Settings pages always include the following functions:

- Email—specifies the SMTP server that XMS uses for sending emails. For details, see [“Web Client—Email Settings” on page 515](#).
- Polling—changes the frequency of polling Arrays. For details, see [“Web Client — Polling Settings” on page 516](#).
- SSH Server—changes the server address provided to Arrays. For details, see [“Web Client — Changing the SSH Server Address” on page 517](#).
- Backup—sets up XMS database backups. For details, see [“Web Client — Database Backup Settings” on page 511](#).

- Server Logs—shows XMS server’s operational logs. For details, see [“Web Client — Viewing Server Log Files” on page 518](#).
- XMS License—manages the license for the XMS software. For details, see [“Web Client—Managing the XMS Server License” on page 520](#).
- About XMS—Click this to display the current running XMS version as well as contact information.

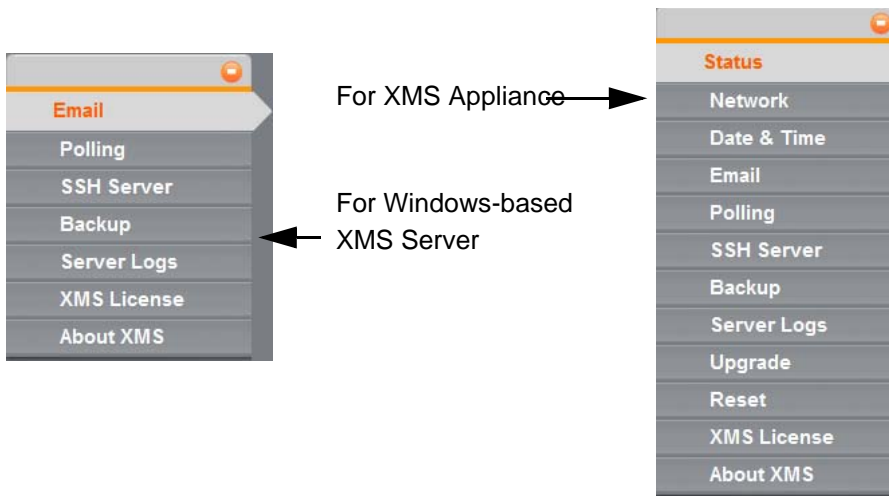


Figure 266. Settings Menus for Windows and Linux Servers

If you have a Linux-based Management Appliance, the following additional choices are offered. Use these pages to manage the appliance, including setting the network address and system date/time:

- Status—Shows the running status of the XMS server. For details, see [“Web Client — Viewing XMS Server Status” on page 506](#).
- Network—Configures IP and other port settings on the Appliance. For details, see [“Web Client — Network Settings” on page 508](#).
- Date & Time—Configures system time on the Appliance. For details, see [“Web Client — Date and Time Settings” on page 509](#).
- Upgrade—Upgrade the XMS server software. For details, see [“Web Client — Performing Upgrades” on page 521](#).

- Reset—Reinitializes the XMS server and database. For details, see [“Web Client — Resetting the XMS Server” on page 522](#).

Dashboard

The web client Dashboard gives you an at-a-glance overview of all system status and activity. Administrators can quickly assess system health and overall system usage, as well as viewing alarm status.

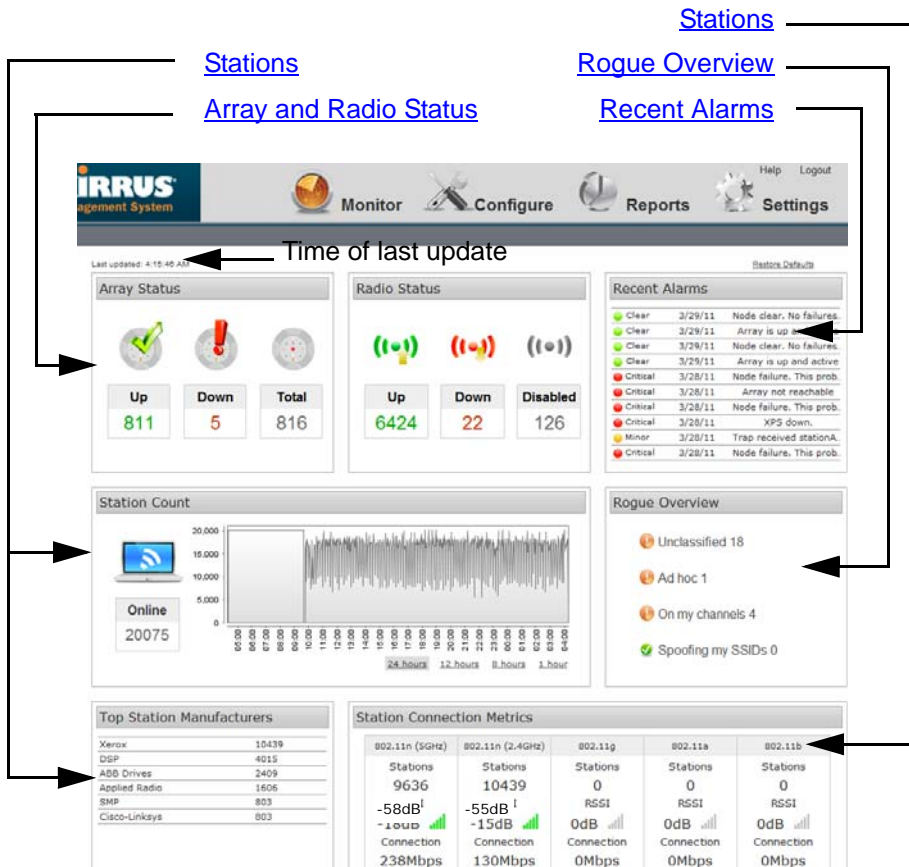


Figure 267. Dashboard

The following sections describe the use of the Dashboard:

- “Dashboard Overview” on page 432
- “About Dashboard Data” on page 432

- [“Array and Radio Status” on page 433](#)
- [“Recent Alarms” on page 435](#)
- [“Stations” on page 436](#)
- [“Rogue Overview” on page 439](#)

Dashboard Overview

When you start the web client, the page starts with the Dashboard displayed. To navigate to it when you have another page displayed, simply click the **Monitor** button at the top of the page and then click **Dashboard** on the left, as indicated in [Figure 262 on page 425](#).

You may rearrange the Dashboard to your liking. Simply click the title bar of one of the sections and drag and drop it to the desired location. Click the **Restore Defaults** link on the upper right to return the layout to its original appearance.

In general, a count is faded if its value is zero. For example, if no Arrays are down in the Array Status section, then the count and its icon are faded. This helps present the at-a-glance health of the Wi-Fi network by eliminating the display of red symbols when there are no devices down.

About Dashboard Data

The Dashboard displays data for all Arrays in the XMS **Managed Network**. The Dashboard is automatically refreshed at frequent intervals—you do not have to refresh explicitly. The time of the most recent update is shown towards the upper left, as seen in [Figure 267](#). Note that some values displayed in the Dashboard may lag with respect to actual current values—items in the XMS database are polled (updated) at differing intervals. When the Dashboard is refreshed, it simply picks up the current values in the database. The XMS server does not poll Arrays to update all status or statistics in the database specifically for a Dashboard refresh. Each data item in the database will be refreshed at whatever rate is defined for it. For more details on the polling rate and how to change it, please see [“Web Client — Polling Settings” on page 516](#) or [“XSMT - Advanced Settings” on page 537](#).

The Dashboard refreshes data at the following rates by default:

- Data for the Dashboard is updated at least every two minutes.
- Alarms occur in real time. Traps generated by Arrays and other events with a severity greater than informational are displayed as alarms.

Array and Radio Status

The Array and Radio Status sections summarize the number of each of these that are up or down.

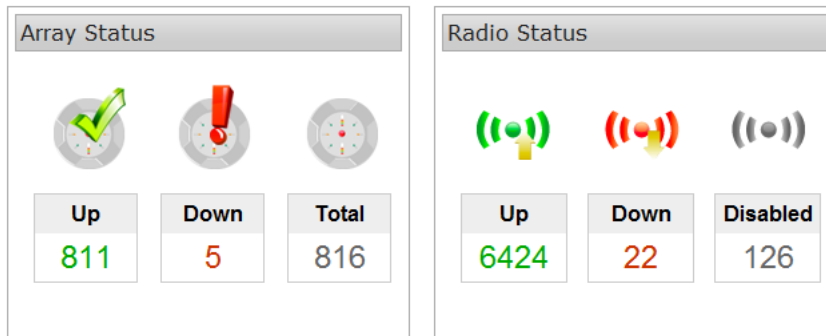


Figure 268. Dashboard - Array and Radio Status

Array Status Details

This is a summary of the status of the Arrays that are known to XMS. The entries show the count of Arrays that are up or down, and the total count. Click on a count, and the web client will display the Arrays or Radios page with only entries that have the status that you selected.

The following status counts are shown:

- **Up (green)**—the number of Arrays that are **up**. Click this button to show only Arrays whose status is up in the Arrays page.
- **Down (red)**—the number of Arrays that are **down**. An Array is considered to be down if XMS has been unable to communicate with it for over three minutes. Click this button to show only Arrays that are down in the Arrays page.

- **Total**—the **total** number of Arrays that are known to XMS. Click this button to show all Arrays in the Arrays page, regardless of status.

Radio Status Details

This is a summary of the status of all radios (IAPs) on Arrays that are known to XMS. The entries show the count of radios at each status value. Each entry is a link—click it to display the **Radios** page, with the IAP list filtered to show only those IAPs that have the selected status value.

The following status counts are shown:

- **Up (green)**—the number of IAPs that are **up**. Click this button to show only IAPs whose status is up in the **Radios** page.
- **Down (red)**—the number of IAPs that are **down**. Click this button to show only IAPs that are down in the **Radios** page.
- **Disabled (gray)**—the number of IAPs that are not enabled on Arrays. Click this button to show only IAPs that are disabled in the **Radios** page.

Recent Alarms

This table lists the most recent alarms generated by your Wi-Fi network. For each alarm, the dashboard shows the severity, the date, and the beginning of the description. To see more information for an alarm in the list, click it to view the Alarm Details. All severity levels are displayed—Critical, Major, Minor, Warning, and Clear.

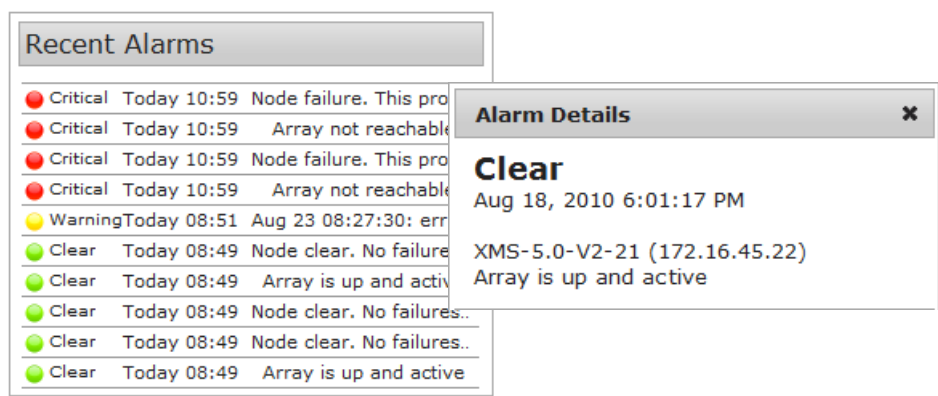


Figure 269. Dashboard - Recent Alarms

To see a complete list of Wi-Fi network alarms, use the web client [Alarms](#) page (see “[Alarms](#)” on page 453) or the Java client [Alarms Window](#) (see “[Alarms](#)” on page 107).

- **Alarm severity classifications**
 - **Critical**—Red
 - **Major**—Orange
 - **Minor**—Gold
 - **Warning**—Yellow
 - **Clear**—Green

Stations

The Stations sections summarize the number of stations associated to Arrays, the proportion using 802.11a, 802.11bg, 802.11b, or 802.11n, list the most numerous station manufacturers for your current network environment, and characterize the quality of those connections in terms of signal strength.

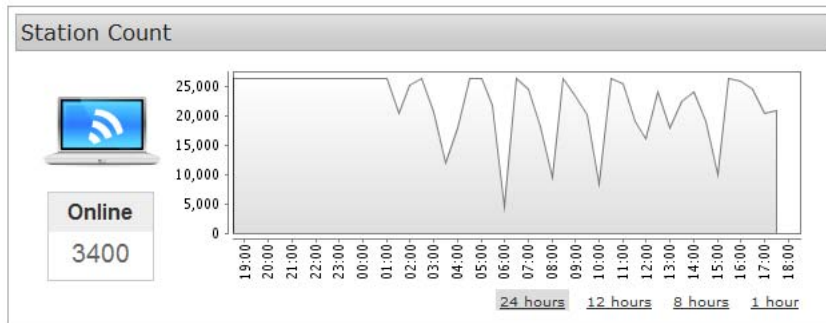


Figure 270. Dashboard - Station Count

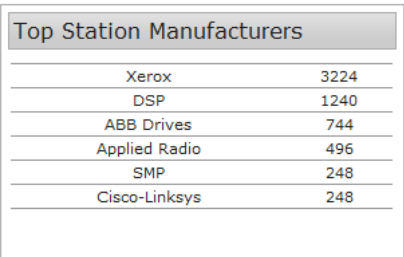
Three sections of the Dashboard describe stations:

- **Station Count Details**
- **Top Station Manufacturers Details**
- **Station Connection Metrics Details**

Station Count Details

This shows the total number of stations associated to Arrays known to XMS, and plots the number of stations over time. (Figure 270) Select the desired time period for the graph— 24 hours is the default.

Top Station Manufacturers Details



Top Station Manufacturers	
Xerox	3224
DSP	1240
ABB Drives	744
Applied Radio	496
SMP	248
Cisco-Linksys	248

Figure 271. Dashboard - Top Station Manufacturers

This provides a breakdown by station manufacturer of the number of stations that are currently associated to Arrays. The most common manufacturers of stations in your network environment are listed, with those having the highest number of stations listed first.

Station Connection Metrics Details

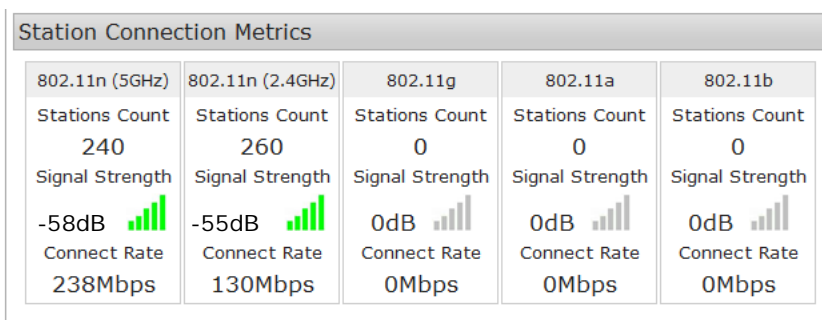


Figure 272. Dashboard - Station Connection Metrics

This section characterizes the average quality of your connections by media type: 802.11n (in the 5GHz and 2.4 GHz bands), 802.11a, 802.11g, and 802.11b stations. For each type of connection, it lists:

- The number of stations.
- The average signal strength of the connections.
- The average actual connection rate.

Rogue Overview

This section provides a quick snapshot of the security status of the Wi-Fi network, including counts of rogue APs. Each entry is a link—click it to display on the selected items on the **Rogues** page.

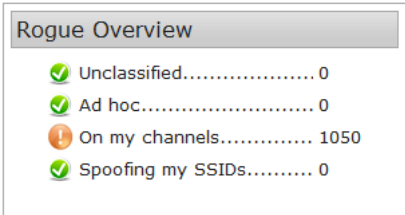


Figure 273. Dashboard - Rogue Overview

For more information about security and intrusion detection, please see **“Security - Managing Intrusions” on page 119**.

This is a summary of the more dangerous APs that have been detected by Arrays. Categories that have a zero count are shown with a green check mark; categories that have a non-zero count are flagged in red. Rogues that you have already classified are not shown. The categories shown are:

- **Unclassified:** When a device is initially detected, it is unclassified, which simply means that no one has classified it yet. Use the Java client to classify a device. See **“About Classifying Detected Devices” on page 120**.
- **Ad hoc:** An ad hoc wireless network is typically a network formed between two or more stations that are communicating with each other directly without going through a normal AP. This line shows a count of ad hoc nodes detected by Array APs. Ad hoc networks can disrupt the performance of your Wi-Fi network by contributing additional RF interference to the environment.
- **On my channels:** This is the number of detected rogues that are on channels that are the same as or adjacent to the channels used by Array radios that are in operation, regardless of the classification of the rogues.

- **Spoofing my SSIDs:** This is the number of detected rogues that are using the same SSIDs as your Wi-Fi network, regardless of the classification of the rogues.

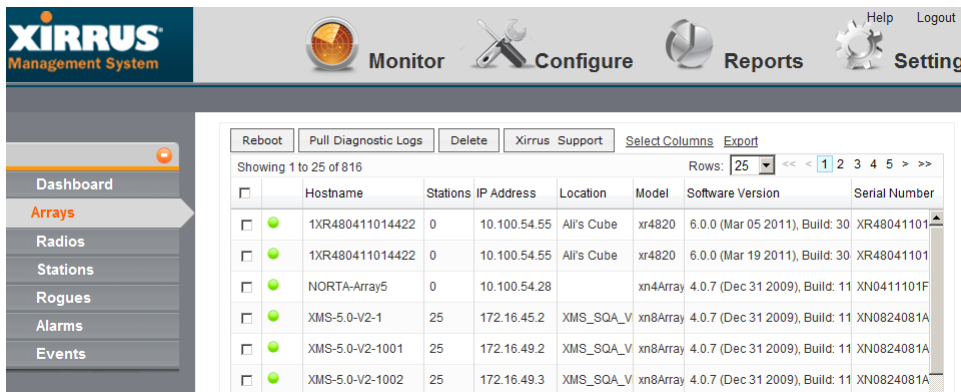
Arrays

The web client Arrays page lists all of the Arrays being managed by XMS, and allows you to perform selected management functions on them. You may reboot Arrays, gather diagnostic logs, or remove Arrays from the XMS database.

The following sections describe the Arrays page:

- [About Using the Arrays Page](#)
- [The Arrays List](#)
- [The Arrays Toolbar](#)

To perform bulk configuration on Arrays, please see [“Network Settings” on page 458](#) and [“Radio Settings” on page 466](#).



	Hostname	Stations	IP Address	Location	Model	Software Version	Serial Number
<input type="checkbox"/>	1XR480411014422	0	10.100.54.55	All's Cube	xr4820	6.0.0 (Mar 05 2011), Build: 30	XR48041101
<input type="checkbox"/>	1XR480411014422	0	10.100.54.55	All's Cube	xr4820	6.0.0 (Mar 19 2011), Build: 30	XR48041101
<input type="checkbox"/>	NORTA-Array5	0	10.100.54.28		xn4Array	4.0.7 (Dec 31 2009), Build: 11	XN0411101F
<input type="checkbox"/>	XMS-5.0-V2-1	25	172.16.45.2	XMS_SQA_V	xn8Array	4.0.7 (Dec 31 2009), Build: 11	XN0824081A
<input type="checkbox"/>	XMS-5.0-V2-1001	25	172.16.49.2	XMS_SQA_V	xn8Array	4.0.7 (Dec 31 2009), Build: 11	XN0824081A
<input type="checkbox"/>	XMS-5.0-V2-1002	25	172.16.49.3	XMS_SQA_V	xn8Array	4.0.7 (Dec 31 2009), Build: 11	XN0824081A

Figure 274. Arrays Page

About Using the Arrays Page

A number of basic operations are available on the Arrays page to allow you to customize it for your own use:

- [Select Columns](#)
- [Export](#)
- [Select Rows](#)
- [Rearranging and Resizing Columns in a Table](#)
- [Sorting](#)

Select Columns

Show or Hide
columns

Rearrange
column
display order

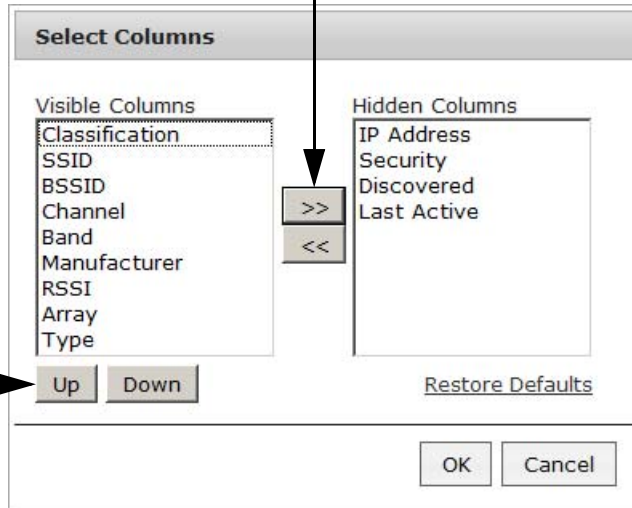


Figure 275. Table Column Chooser

The page may be customized by changing the columns that are displayed and the order of display. If you prefer to use a smaller browser window for XMS and there's not enough room for all the columns to display, you can use this feature to select your preferred columns. Click the **Select Columns** link on the upper right to display the table column chooser.

The **Visible Columns** list shows the columns that will be displayed. To hide a column, select it from the Visible Columns and click >> to move it to the **Hidden Columns** list. Similarly, to display a column, select it from the Hidden Columns and click << to move it to the Visible Columns list. There is also a button to **Restore Default** column display. Use the **Up** and **Down** buttons to arrange the columns, left to right. Click **OK** when done.

These changes are persistent for a user—if you log out, they will still apply the next time that you open the web client.

Export

The **Export** link above the list may be used to export rows from this page to an Excel file or to a CSV file—a set of comma-separated values that are compatible with Microsoft Excel. The exported file may be used to provide Xirrus Customer Support with a snapshot of the configuration of your network, at their request.

All rows will be exported, regardless of whether you have selected only a subset of entries.

When you click **Export**, a dialog box allows you to select the file format. Click the **Export** button again to browse to the destination folder and specify the filename. You may choose to save the results in a file or open them in Excel. Close the Export dialog when done.

Select Rows

Simply click the checkboxes of the rows you wish to select. You may then click function buttons to perform operations on the selected entries. You may click the checkbox in the header row to select all rows. Click again to deselect all rows.

If the list contains multiple pages of information, use the browse buttons provided on the far right above the list to navigate between pages. Use << or >> to jump to the first page or last page, respectively.

Rearranging and Resizing Columns in a Table

For easier viewing of list data, you may rearrange columns by dragging the column header and moving it to the desired position. This is helpful if you wish to view particular columns in close proximity, or to move less viewed columns to the right. The new arrangement is saved per user. The next time you log in, you will see the columns in the same order.

To resize a column, simply drag the right-side edge of the column to expand or reduce the width of the column.

Sorting

To change how the table is sorted, click in any column header to define that column as the sort criteria. In addition, you can choose to have the results

displayed in ascending order or descending order. To do this, simply click in the same header again to toggle between ascending and descending order.

The Arrays List

The Arrays List ([Figure 274 on page 441](#)) shows Arrays that have been discovered by XMS. You may customize the columns shown in this list—see [“Select Columns” on page 442](#). This list is very similar to the [“Arrays Window” on page 166](#). Note that the Arrays Window offers different capabilities, such as filtering to display a subset or group of Arrays, searching for Arrays, viewing performance, and more management operations.

For each Array, the following information is shown by default:

- The current **Status** of each Array
- The **Array Host Name**
- The **Gig1 IP Address** of the Array
- The **Location** of the Array (if this information was configured on the Array)
- The **Model** of the Array
- The number of **Stations** associated to this Array
- The **Software Version** currently running on the Array

The Arrays Toolbar

The Arrays toolbar allows you to gather diagnostic information for Array management. This function is only available on this page (it is not offered on the **Arrays Window**). The toolbar also allows you to reboot selected Arrays or delete Arrays from the XMS database.

To perform configuration on multiple Arrays at one time, please see “**Network Settings**” on page 458 and “**Radio Settings**” on page 466.

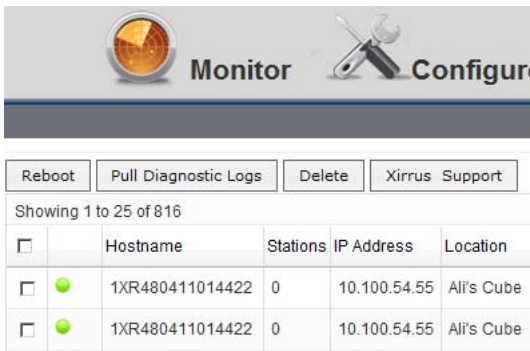


Figure 276. The Array Page Toolbar

Select one or more Arrays in the list by clicking their checkboxes in the first column. You may click the checkbox in the header row to select all Arrays, or click again to deselect all. The following operations are available:

- **Reboot**—this option reboots the selected Arrays. You will be asked to confirm the operation.
- **Pull Diagnostic Logs**—this option initiates a task that instructs the selected Arrays to create a diagnostic log file. When the diagnostic log is complete, a link will appear. Click it to download the requested diagnostic results as a zip file.

Pulling diagnostic logs from 8 array(s). This operation will take about 2 minutes to complete. When the download link appears below, you can download the logs.

[Download Diagnostic Logs](#)

Figure 277. Pull Diagnostic Logs

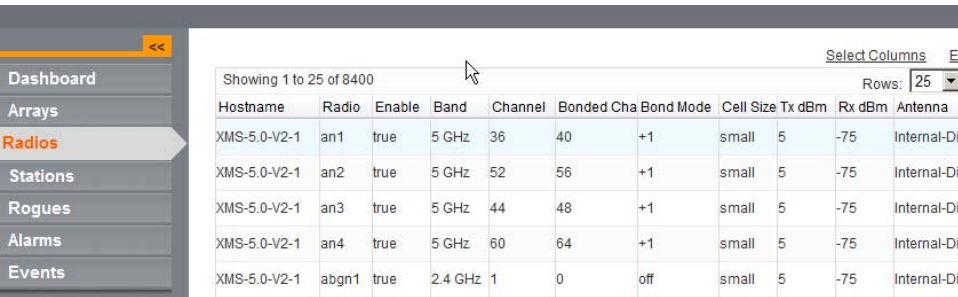
- **Delete**—this option removes the selected Arrays from the XMS database. You will be asked to confirm the operation.
- **Xirrus Support**—this button is an example of a function added with the **Custom Actions** page.

Radios

The web client Radios page lists the radios (IAPs) on all of the Arrays being managed by XMS. This is a display-only page, but values may be exported.

The following sections describe the Radios page:

- [About Using the Radios Page](#)
- [The Radios List](#)



Showing 1 to 25 of 8400											Select Columns	Export
											Rows: 25	
Hostname	Radio	Enable	Band	Channel	Bonded Cha	Bond Mode	Cell Size	Tx dBm	Rx dBm	Antenna		
XMS-5.0-V2-1	an1	true	5 GHz	36	40	+1	small	5	-75	Internal-Di		
XMS-5.0-V2-1	an2	true	5 GHz	52	56	+1	small	5	-75	Internal-Di		
XMS-5.0-V2-1	an3	true	5 GHz	44	48	+1	small	5	-75	Internal-Di		
XMS-5.0-V2-1	an4	true	5 GHz	60	64	+1	small	5	-75	Internal-Di		
XMS-5.0-V2-1	abgn1	true	2.4 GHz	1	0	off	small	5	-75	Internal-Di		

Figure 278. Radios Page

About Using the Radios Page

A number of basic operations are available on the Radios page to allow you to customize it for your own use:

- [“Select Columns” on page 442](#)
- [“Export” on page 443](#)
- [“Rearranging and Resizing Columns in a Table” on page 443](#)
- [“Sorting” on page 443](#)

The Radios List

The Radios List ([Figure 278 on page 447](#)) shows all of the radios on Arrays that have been discovered by XMS. You may customize the columns shown in this list—see [“Select Columns” on page 442](#). This list is very similar to the list on the [“IAPs Window” on page 198](#). Note that the [IAPs Window](#) offers different capabilities, such as filtering to display only radios belonging to a subset or group of Arrays, searching, viewing performance, and management operations.

For each radio, the following information is shown by default. Please see [“IAP Setting Details \(Figure 203\)” on page 311](#) for a detailed description of these fields.

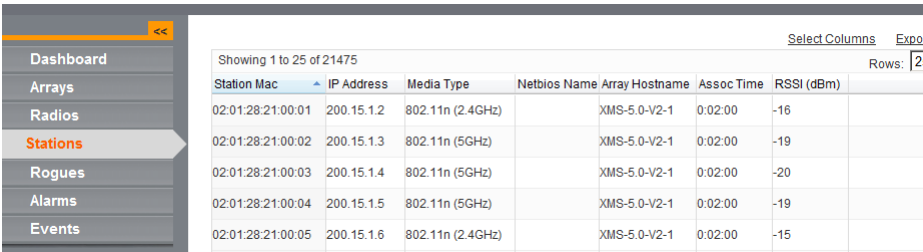
- The **Hostname**.
- The **Radio** name (e.g., abgn2, an3, etc.).
- Whether the radio is **Enabled**.
- The **Band** that the radio is using.
- The radio’s current **Channel** number.
- For IEEE 802.11n radios, the **Bonded Channel** for this radio.
- For IEEE 802.11n radios, the **Bond Mode** that was set for this radio.
- The radio’s current **Cell Size**.
- The radio’s current **Tx dBm** (transmit power) setting.
- The radio’s current **Rx dBm** (receive threshold) setting.
- The radio’s current **Antenna** setting (internal or external).

Stations

The web client Stations page lists the stations that are associated to all Arrays within your managed network. This is a display-only page, but values may be exported.

The following sections describe the Stations page:

- [About Using the Stations Page](#)
- [The Stations List](#)



Station Mac	IP Address	Media Type	Netbios Name	Array Hostname	Assoc Time	RSSI (dBm)
02:01:28:21:00:01	200.15.1.2	802.11n (2.4GHz)		XMS-5.0-V2-1	0:02:00	-16
02:01:28:21:00:02	200.15.1.3	802.11n (5GHz)		XMS-5.0-V2-1	0:02:00	-19
02:01:28:21:00:03	200.15.1.4	802.11n (5GHz)		XMS-5.0-V2-1	0:02:00	-20
02:01:28:21:00:04	200.15.1.5	802.11n (5GHz)		XMS-5.0-V2-1	0:02:00	-19
02:01:28:21:00:05	200.15.1.6	802.11n (2.4GHz)		XMS-5.0-V2-1	0:02:00	-15

Figure 279. Stations Page

About Using the Stations Page

A number of basic operations are available on the Stations page to allow you to customize it for your own use:

- [“Select Columns” on page 442](#)
- [“Export” on page 443](#)
- [“Rearranging and Resizing Columns in a Table” on page 443](#)
- [“Sorting” on page 443](#)

The Stations List

The Stations List ([Figure 279 on page 449](#)) shows all of the stations associated to Arrays that have been discovered by XMS. You may customize the columns shown in this list—see [“Select Columns” on page 442](#). This list is very similar to list on the [“Stations Window” on page 203](#).

This list shows information about each station and the IAP to which it is associated. For each station, the following information is shown by default:

- The **Station MAC** address.
- The **IP Address** of the station.
- The **Media Type** supported by the station: 802.11n (5 GHz or 2.4 GHz), 802.11a, 802.11b, or 802.11bg.
- The **NetBIOS** name of the station.
- The **Array Host Name** of the Array to which the station is associated.
- The **Assoc Time**—How long (in days:hours:minutes) the station has been associated to the Array.
- The current **RSSI** (signal strength) of the connection as measured by the radio.

Rogues

The web client Rogues page lists the potential rogue access points detected by Arrays in the network, and types of encryption in use. The Arrays that detected the intruding APs are also identified. This is a display-only page, but values may be exported.

The following sections describe the Rogues page:

- [About Using the Rogues Page](#)
- [The Rogues List](#)

Select ColumnsExport

Showing 1 to 25 of 25											
Classification	SSID	BSSID	Channel	Band	Manufacturer	RSSI	Array	Type	Security	Discovered	Last Active
Known	wds-link	00:0f:7d:04:23:a1	11	2.4 GHz	Xirrus	-57	XMS-5.0-V2-508	Infrastructure	none	2/4/17	2/28/17
Known	SQAWPA	00:0f:7d:04:23:a2	11	2.4 GHz	Xirrus	-64	XMS-5.0-V2-508	Infrastructure	AES+TKIP+EAP	2/4/17	2/28/17
Known	SQAWPR8	00:0f:7d:04:23:a0	11	2.4 GHz	Xirrus	-65	XMS-5.0-V2-508	Infrastructure	none	2/4/17	2/28/17
Known	L3R-Open	00:0f:7d:00:89:a0	6	2.4 GHz	Xirrus	-58	XMS-5.0-V2-508	Infrastructure	none	2/4/17	2/28/17
Known	S16Open	00:0f:7d:00:89:d4	48	5 GHz	Xirrus	-60	XMS-5.0-V2-508	Infrastructure	none	2/4/17	2/28/17
Known	L3R-EAP	00:0f:7d:00:89:d1	48	5 GHz	Xirrus	-59	XMS-5.0-V2-508	Infrastructure	AES+EAP	2/4/17	2/28/17

Figure 280. Rogues Page

About Using the Rogues Page

A number of basic operations are available on the Rogues page to allow you to customize it for your own use:

- [“Select Columns” on page 442](#)
- [“Export” on page 443](#)
- [“Rearranging and Resizing Columns in a Table” on page 443](#)
- [“Sorting” on page 443](#)

The Rogues List

The Rogues List (**Figure 280 on page 451**) shows all of the rogues that have been detected by XMS. You may customize the columns shown in this list—see **“Select Columns” on page 442**. This list is very similar to the one in the **“The Devices Window” on page 119**. Note that the **The Devices Window** offers additional capabilities, such as filtering to display only rogues with a particular classification or only those that have been detected by a group of Arrays, searching, classification operations, and creating classification rules.

This list shows information about each rogue and the Array which detected it. For each rogue, the following information is shown by default:

- The rogue’s **Classification** (**Unclassified, Approved, Known, Blocked, or Unknown**). See **“Detected Devices” on page 123** for an explanation of the categories.
- The rogue’s **SSID**.
- The rogue’s **BSSID** (MAC address).
- The **Channel** being used for the connection.
- The **Band** (5 GHz or 2.4 GHz) being used for the connection.
- The **Manufacturer** of the rogue device.
- The current **RSSI** (signal strength) of the rogue’s signal as measured by the Array that detected it.
- The host name of the **Array** that detected the rogue.
- The **Type** of the rogue's wireless network - Ad Hoc or Infrastructure.

Alarms

The web client Alarms page lists the alarms received by XMS. All alarm levels are displayed—Critical, Major, Minor, Warning, and Clear. This is a display-only page, but values may be exported.

Showing 11 to 20 of 26						Select Columns	Export
Time	Severity	Source Mac	IP Address	Hostname	Description		
Oct 10, 2010 11:13:47 PM	Clear	00:0f:7d:00:03:1f	10.100.54.111	XS0834081AA38	Array is up and active		
Oct 10, 2010 11:13:47 PM	Clear	00:0f:7d:00:03:1f	10.100.54.111	XS0834081AA38	Node clear. No failures on this node.		
Oct 11, 2010 10:16:38 AM	Warning	00:0f:7d:00:42:9b	10.100.54.37	XS_39-10.100.40.37	Oct 11 10:44:56: alert : Rogue AP detected. SSID: L3R-Open, BSSID:		
Oct 11, 2010 10:20:59 AM	Clear	00:0f:7d:00:91:7a	10.100.54.26	Robin-XN8	Array is up and active		
Oct 11, 2010 10:20:59 AM	Clear	00:0f:7d:00:91:7a	10.100.54.26	Robin-XN8	Node clear. No failures on this node.		

Figure 281. Alarms Page

The following sections describe the Alarms page:

- [About Using the Alarms Page](#)
- [The Alarms List](#)

About Using the Alarms Page

A number of basic operations are available on the Alarms page to allow you to customize it for your own use:

- [“Select Columns” on page 442](#)
- [“Export” on page 443](#)
- [“Rearranging and Resizing Columns in a Table” on page 443](#)
- [“Sorting” on page 443](#)

The Alarms List

The Alarms List ([Figure 281](#)) shows the alarms that have been received by XMS. You may customize the columns shown in this list—see [“Select Columns” on page 442](#). This list is very similar to the one in [“Alarms” on page 107](#). Note that the Java client’s [Alarms Window](#) offers additional capabilities that are not available on this page, such as filtering to display only alarms with a particular

severity. Only the current (most recent) alarm in each category for each device will be shown in this list.

This list shows information about each alarm and the Array that generated it. For each alarm, the following information is shown by default:

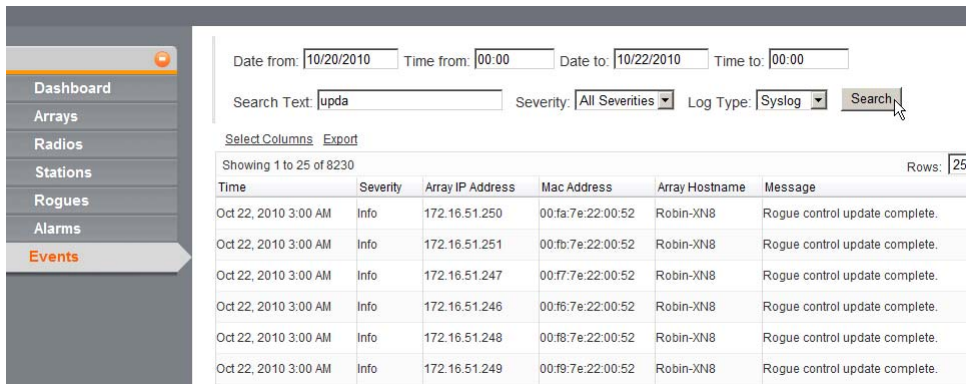
- The **Time** and date of the alarm.
- The alarm's **Severity** (**Critical**, **Major**, **Minor**, **Warning**, or **Clear**). See [“Alarms” on page 107](#) for more details.
- The **Source MAC** address of the Array that generated the alarm.
- The **IP Address** of the Array that generated the alarm.
- The **Hostname** of the Array that generated the alarm.
- A text **Description** of the alarm.

Events

The web client Events page lists the log and syslog messages received by XMS. All severity levels above the informational level are shown by default. This is a display-only page, but values may be exported. A set of search fields above the list allow you to select the messages to be displayed.

For the XMS syslog to function well, Arrays must meet certain requirements, such as being configured to use an NTP server for setting system time. Please see [“Syslog Events” on page 112](#) for details.

The Events page has a special search feature for finding particular log messages. This is described in [“About Using the Events Page” on page 455](#).



Time	Severity	Array IP Address	Mac Address	Array Hostname	Message
Oct 22, 2010 3:00 AM	Info	172.16.51.250	00:1a:7e:22:00:52	Robin-XN8	Rogue control update complete.
Oct 22, 2010 3:00 AM	Info	172.16.51.251	00:1b:7e:22:00:52	Robin-XN8	Rogue control update complete.
Oct 22, 2010 3:00 AM	Info	172.16.51.247	00:17:7e:22:00:52	Robin-XN8	Rogue control update complete.
Oct 22, 2010 3:00 AM	Info	172.16.51.246	00:16:7e:22:00:52	Robin-XN8	Rogue control update complete.
Oct 22, 2010 3:00 AM	Info	172.16.51.248	00:18:7e:22:00:52	Robin-XN8	Rogue control update complete.
Oct 22, 2010 3:00 AM	Info	172.16.51.249	00:19:7e:22:00:52	Robin-XN8	Rogue control update complete.

Figure 282. Events Page

The following sections describe the Events page:

- [About Using the Events Page](#)
- [The Events List](#)

About Using the Events Page

A number of basic operations are available on the Events page to allow you to customize it for your own use:

- [“Select Columns” on page 442](#)
- [“Export” on page 443](#)

- [“Rearranging and Resizing Columns in a Table” on page 443](#)
- [“Sorting” on page 443](#)

The Events page has a number of search fields that allow you to filter the log messages to be displayed. This is a very useful feature, since the list may contain a large number of messages. To search for the desired messages, use any or all of the following fields:

- Specify a time period (optional)—enter the **Date from/Time from** and/or **Date to/Time to** fields. The Dates are entered by clicking in the field and selecting the desired date from the popup calendar, or by typing the date in **mm/dd/yyyy** format. Times are specified by clicking in the field and using the drag bars to select the **Hour** and **Minute**.
- Enter **Search Text** (optional)—XMS will search for entries that contain this text in any position in any field.
- Select the desired **Severity**. If you select a particular severity level, *only* messages at that level will be displayed (rather than displaying messages at that level and above). The default value is **All Severities**, which shows all messages at the informational level and above.
- Select the **Log Type**. The default is All Logs, which displays all XMS log files including syslog messages.

The Events List

The Events List ([Figure 281](#)) shows the events that have been received by XMS. You may customize the columns shown in this list—see [“Select Columns” on page 442](#). This list is very similar to the one in [“Events” on page 111](#).

This list shows information about each event and the Array that generated it. For each event, the following information is shown by default:

- The **Time** and date of the event.
- The event’s **Severity**. See [“Syslog Severity Levels” on page 113](#) for more details.
- The **Array IP Address** of the Array that generated the event.
- The **MAC Address** of the Array that generated the event.

- The **Array Hostname** of the Array that generated the event.
- The **Message**—a text description of the event.

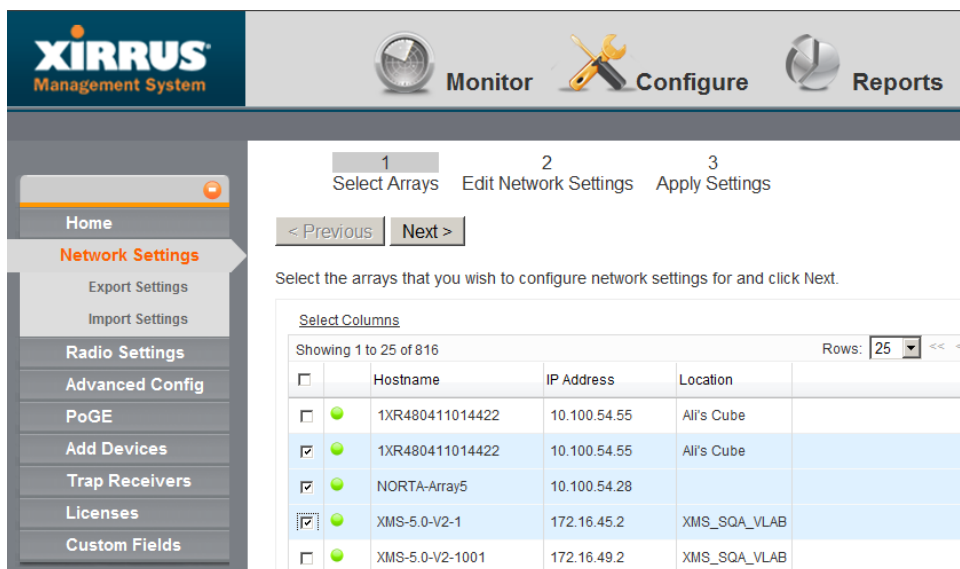
Configure—Home Page

This page lists the Arrays in the XMS database and allows you to reboot or delete the selected Arrays, or fetch diagnostic information. This page is identical to the Monitor—Arrays page. Please see “[Arrays](#)” on page 441.

Network Settings

The Network Settings page provides very convenient options for configuring certain Array network settings. Some of these functions are also available from the [Arrays Window](#), and some, like bulk configuration (as described below in [To Modify Multiple Rows](#)) are available only from this web client window. Bulk configuration is a particularly valuable feature, allowing you to change network settings on a number of Arrays in one step.

Open the Network Settings page by clicking the **Configure** button near the top of the window, then select **Network Settings** on the left.



	Hostname	IP Address	Location
<input type="checkbox"/>	1XR480411014422	10.100.54.55	Ali's Cube
<input checked="" type="checkbox"/>	1XR480411014422	10.100.54.55	Ali's Cube
<input checked="" type="checkbox"/>	NORTA-Array5	10.100.54.28	
<input checked="" type="checkbox"/>	XMS-5.0-V2-1	172.16.45.2	XMS_SQA_VLAB
<input type="checkbox"/>	XMS-5.0-V2-1001	172.16.49.2	XMS_SQA_VLAB

Figure 283. Network Settings Page

You may use this page **To Modify Rows Individually**, or choose **To Modify Multiple Rows** for bulk configuration—this applies identical settings to the selected rows (except for the IP Address, which is used as a starting point for a range of addresses). You may also choose **To Export Network Settings**, and possibly **To Import Network Settings** after making changes to them.

About Using the Network Settings Page

A number of basic operations are available on this page to allow you to customize it for your own use:

- **“Select Columns” on page 442**
- **“Rearranging and Resizing Columns in a Table” on page 443**
- **“Sorting” on page 443**



*Exporting - note that any time you click the **Export** button or use the **Export Settings** link, the old unedited values will be exported, unless you have completed saving your edited values to the Arrays.*

To Modify Rows Individually

1. **Step 1 - Select Arrays:** For each row that you wish to modify, select the checkbox at the beginning of the row. Click the checkbox in the header row to select all rows. Click again to deselect all rows.

Click **Next>** when the desired rows are selected.

2. **Step 2 - Edit Network Settings:** You may edit the values in the following columns: **Hostname**, **Gig1 DHCP**, **Gig1 IP Address**, **Gig1 Mask**, **Gig1 Gateway**, **Location**. Simply click a table cell that you wish to modify. A text box will be displayed where you may type the desired value. **(Figure 284)** You may change as many cells in as many rows as you wish. There is no need to click the check boxes on modified rows. Modifications will be highlighted on the page.

Click **Finish** when done.

1
Select Arrays
2
Edit Network Settings
3
View Results

< Previous
Finish
Cancel

Click on a value below to edit an individual Array's settings or select multiple rows and click "Bulk Edit" to edit multiple Arrays at once. Once you are done with your changes click "Finish" to apply your settings to the Arrays.

Bulk Edit
Select Columns Export

Showing 1 to 3 of 3

<input type="checkbox"/>	Gig1 Mac Address	Serial Number	Hostname	Gig1 DHCP	Gig1 IP Address	Gig1 Mask	Gig1 Gateway	Location	Row
<input type="checkbox"/>	00:0b:7e:16:00:52	XN0824081A2E2	XMS-5.0-V2-10			255.255.0.0	200.200.1.1	XMS_SQA_VLAB	
<input type="checkbox"/>	00:65:7e:16:00:52	XN0824081A2E2				255.255.0.0	200.200.1.1	XMS_SQA_VLAB	
<input type="checkbox"/>	00:66:7e:16:00:52	XN0824081A2E2	XMS-5.0-V2-101	true	200.200.45.102	255.255.0.0	200.200.1.1	XMS_SQA_VLAB	

Figure 284. Editing the Network Settings Page

- Step 3 - View Results:** The web client will apply the changes you entered, and display the success or failure of the configuration operation on the selected Arrays.

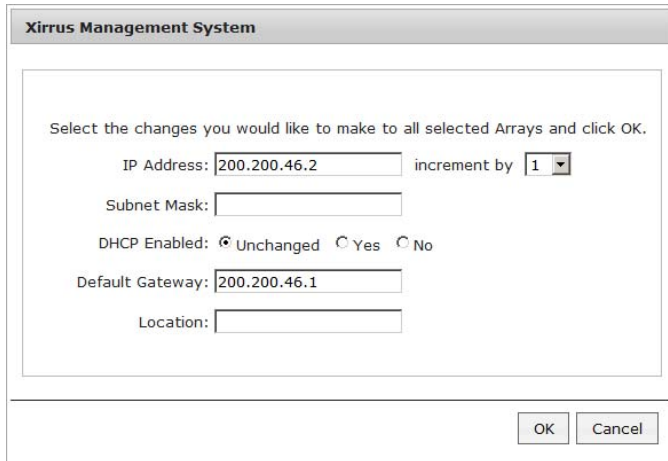
To Modify Multiple Rows

Use this procedure to quickly configure multiple Arrays to have the same settings. A range of IP addresses may be assigned to the Arrays—Bulk Edit will prevent you from making the mistake of assigning identical IP addresses to multiple Arrays.

- Step 1 - Select Arrays:** For each row that you wish to modify, select the checkbox at the beginning of the row. To select all rows, click the checkbox in the header row. Click again to deselect all rows.

Click **Next>** when the desired rows are selected.

- Step 2 - Edit Network Settings:** Select the rows that you wish to edit by clicking their check boxes. Then click the **Bulk Edit** button. This displays blank fields for all of the settings that are modifiable in bulk): **IP Address, Increment, Subnet Mask, DHCP Enabled, Default Gateway, Location.** (Figure 285)



The image shows a screenshot of the 'Xirrus Management System' Bulk Configuration dialog box. The title bar reads 'Xirrus Management System'. Inside the dialog, there is a text instruction: 'Select the changes you would like to make to all selected Arrays and click OK.' Below this, there are several input fields: 'IP Address' with the value '200.200.46.2', 'Subnet Mask' (empty), 'Default Gateway' with the value '200.200.46.1', and 'Location' (empty). To the right of the 'IP Address' field is a label 'increment by' followed by a dropdown menu showing the value '1'. Below the 'IP Address' field is a label 'DHCP Enabled' with three radio buttons: 'Unchanged' (selected), 'Yes', and 'No'. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

Figure 285. Bulk Configuration (Network Settings)

For the **IP Address** field, enter the starting value for a range of addresses. Then select an **Increment by** value for the range. Note that Array host names cannot be bulk configured. Bulk edit fields that are left blank will be unchanged on Arrays.

Click **OK** when done. The Bulk Edit dialog closes, and your desired changes will be displayed in the network settings table. Note that the new values have not yet been sent to the Arrays. Take a moment to review your changes. In particular, make sure that the IP addresses that were assigned are correct. You may individually edit any incorrect settings.

Click **Finish** when satisfied with the changes.

3. **Step 3 - View Results:** The web client will apply the changes you entered, and display the success or failure of the configuration operation on the selected Arrays.

To Export Network Settings

This option exports IP and other network settings on selected Arrays to an Excel file or to a CSV file—a set of comma-separated values that are compatible with Microsoft Excel. This file is useful in a number of ways:

- As a backup of the current configuration, especially since the settings in the file may be imported to restore this configuration.
- To provide Xirrus Customer Support with a snapshot of the configuration of your network, at their request.
- You may edit the settings in this file and then import the changed values. Take care only to modify the fields that are editable on the Bulk Configuration page.

To import a file that was exported from the Network Settings page, see [“To Import Network Settings” on page 464](#).

Note that any time you click the **Export** button or use the **Export Settings** link, the old unedited values will be exported, unless you have completed saving your edited values to the Arrays.

1. **Step 1 - Select Arrays:** Open the Network Settings page by clicking the **Configure** button near the top of the window, then select **Network Settings** on the left. Click the **Export Settings** link that appears underneath.

For each row that you wish to export, select the checkbox at the beginning of the row. To select all rows, click the checkbox in the header row. Click again to deselect all rows. (Figure 287) Click **Next>** when the desired rows are selected.

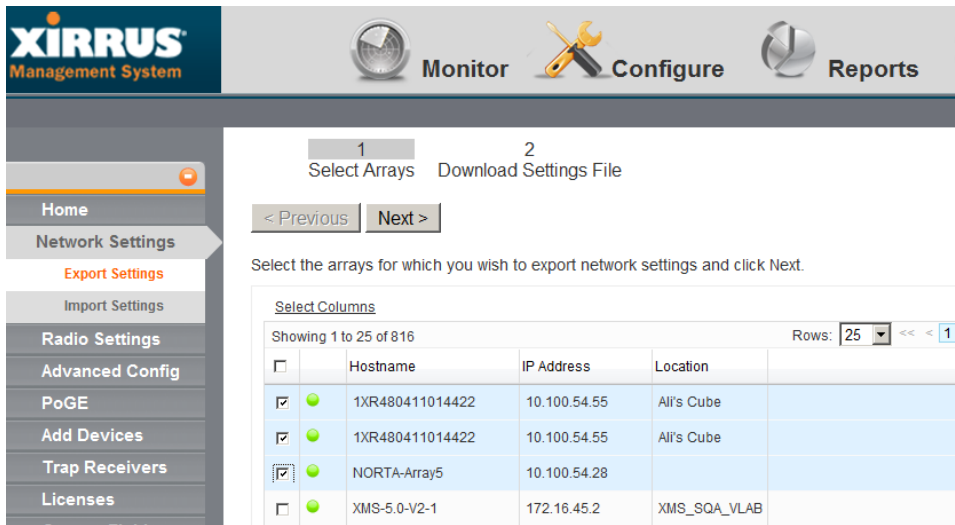
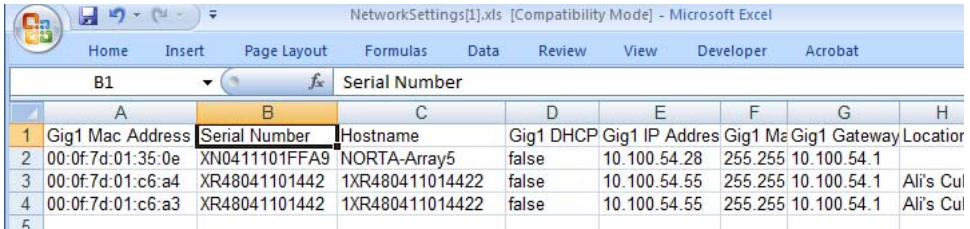


Figure 286. Export Network Settings

- Step 2 - Download Settings File:** Select the desired output file format: Excel or CSV. Click the **Export** button again to browse to the destination folder and specify the filename. (Figure 287)



	A	B	C	D	E	F	G	H
	Gig1 Mac Address	Serial Number	Hostname	Gig1 DHCP	Gig1 IP Address	Gig1 Mask	Gig1 Gateway	Location
1	00:0f:7d:01:35:0e	XN0411101FFA9	NORTA-Array5	false	10.100.54.28	255.255.255.255	10.100.54.1	
2	00:0f:7d:01:c6:a4	XR48041101442	1XR480411014422	false	10.100.54.55	255.255.255.255	10.100.54.1	Ali's Cul
3	00:0f:7d:01:c6:a3	XR48041101442	1XR480411014422	false	10.100.54.55	255.255.255.255	10.100.54.1	Ali's Cul

Figure 287. Exported Network Settings File

- You may choose to save the results in a file or open them in Excel. Click **Cancel** when done to close the Export dialog.

To Import Network Settings

This option allows you to change IP and other network settings on Arrays by importing a file that was exported from the Network Settings page. See [“To Export Network Settings” on page 461](#) for instructions on exporting settings to a file.

1. **Step 1 - Upload Settings File:** Open the Network Settings page by clicking the **Configure** button near the top of the window, then select **Network Settings** on the left. Click the **Import Settings** link that appears underneath.

Click **Choose File**, and browse to the desired .xls or .csv file. (Figure 288) Next, click the **Upload** button.

Click **Next>** when the **Upload Complete** message appears.

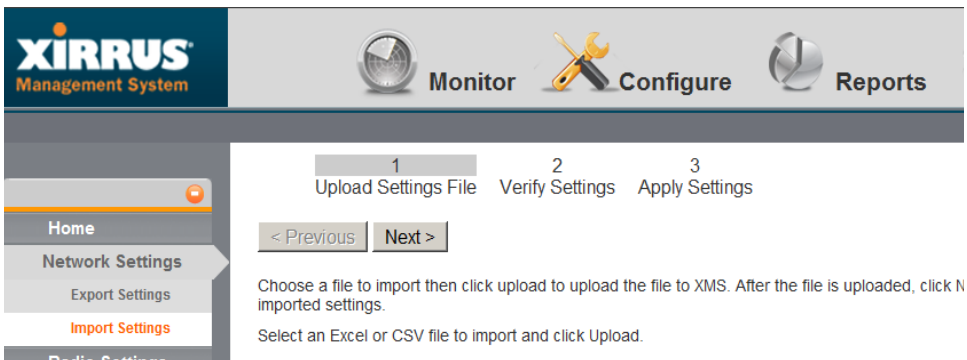


Figure 288. Import Network Settings

2. **Step 2 - Verify Settings:** This page lists network settings for all of the Arrays that were included in the imported file. (Figure 289) Review these values carefully. Click a setting to change it. An edit field will appear if the setting is modifiable. There is also a **Bulk Edit** option which may be used as described in [“To Modify Multiple Rows” on page 460](#).

Click the **Finish** button when you are done making changes.

1

2

3

Upload Settings File

Verify Settings

Apply Settings

< Previous

Finish

Cancel

Verify the imported settings below. You can also make additional changes at this time. When you are ready to apply your settings click Finish.

Bulk Edit

Select Columns

Showing 1 to 3 of 3

Row

<input type="checkbox"/>	Gig1 Mac Address	Serial Number	Hostname	Gig1 DHCP	Gig1 IP Address	Gig1 Mask	Gig1 Gateway	Location
<input checked="" type="checkbox"/>	01:61:7e:21:00:52	XN0824081A2E2	XMS-5.0-V2-1351	true	200.200.50.102	255.255.0.0	200.200.1.1	XMS_SQA
<input checked="" type="checkbox"/>	01:62:7e:21:00:52	XN0824081A2E2	XMS-5.0-V2-1352	<div>true</div>	200.200.50.103	255.255.0.0	200.200.1.1	XMS_SQA
<input type="checkbox"/>	01:63:7e:21:00:52	XN0824081A2E2	XMS-5.0-V2-1353	true	200.200.50.104	255.255.0.0	200.200.1.1	XMS_SQA

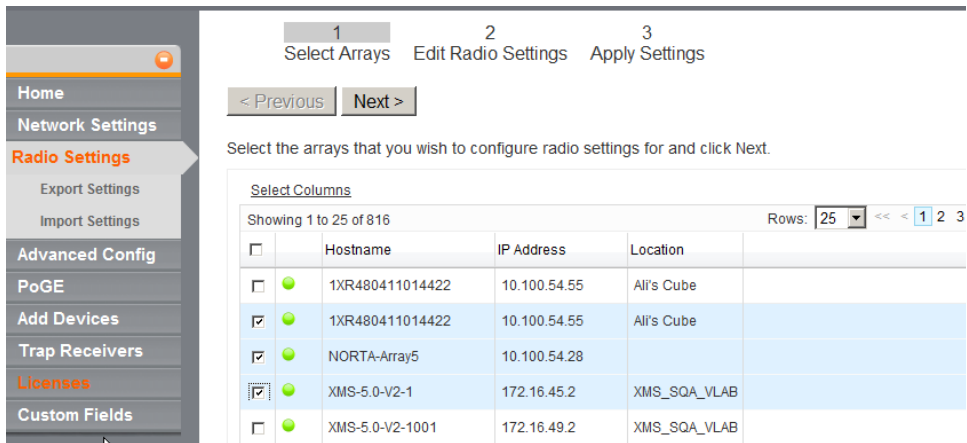
Figure 289. Verify Imported Network Setting Values

3. **Step 3 - Apply Settings:** The web client will apply the changes you entered, and display the success or failure of the configuration operation on the selected Arrays.

Radio Settings

The Radio Settings configuration page provides very convenient options for configuring settings on a per-radio (IAP) basis. Some of these functions are also available from the **IAPs Window**, but bulk configuration and the ability to set different values on multiple radios easily at one time are available only from this web client window. Bulk configuration is a particularly valuable feature, allowing you to apply the same settings to multiple radios in one step.

Open this configuration page by clicking the **Configure** button near the top of the window, then select **Radio Settings** on the left.



Select Columns			Showing 1 to 25 of 816		Rows: 25	<<	<	1	2	3
<input type="checkbox"/>		Hostname	IP Address	Location						
<input type="checkbox"/>		1XR480411014422	10.100.54.55	Ali's Cube						
<input checked="" type="checkbox"/>		1XR480411014422	10.100.54.55	Ali's Cube						
<input checked="" type="checkbox"/>		NORTA-Array5	10.100.54.28							
<input checked="" type="checkbox"/>		XMS-5.0-V2-1	172.16.45.2	XMS_SQA_VLAB						
<input type="checkbox"/>		XMS-5.0-V2-1001	172.16.49.2	XMS_SQA_VLAB						

Figure 290. Radio Settings Page

You may use this page **To Modify Rows Individually**, or choose **To Modify Multiple Rows** for bulk configuration—this applies identical settings to the selected rows. You may also choose **To Export Radio Settings**, and possibly **To Import Radio Settings** after making changes to them.

Please see **“IAP Setting Details (Figure 203)” on page 311** for a detailed description of the settings shown on this page.

Note that any time you click the **Export** button or use the **Export Settings** link, the old unedited values will be exported, unless you have completed saving your edited values to the Arrays.

To Modify Rows Individually

- 1. **Step 1 - Select Arrays:** For each radio that you wish to modify, select the checkbox at the beginning of the row. Click the checkbox in the header row to select all rows. Click again to deselect all rows.

Click **Next>** when the desired rows are selected.

- 2. **Step 2 - Edit Radio Settings:** You may edit the values in the following columns: **Enable**, **Band**, **Channel**, **Bonded Channel**, **Bond Mode**, **Locked**, **Cell Size**, **Tx dBm**, **Rx dBm**, and **Antenna**. Simply click a table cell that you wish to modify. A text box will be displayed where you may type the desired value, then click **OK**. (Figure 284) You may change as many cells in as many rows as you wish. There is no need to click the check boxes on modified rows. Modifications will be highlighted on the page.

Click **Finish** when done.

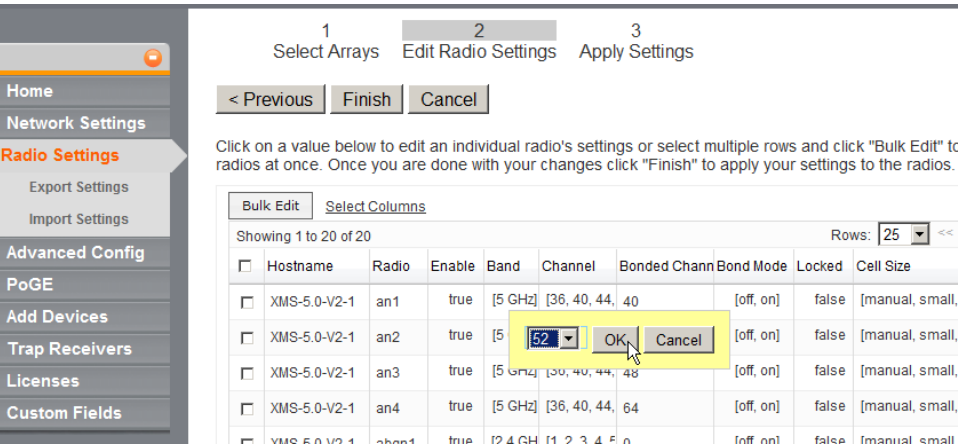


Figure 291. Editing the Radio Settings Page

- 3. **Step 3 - View Results:** The web client will apply the changes you entered, and display the success or failure of the configuration operation on the selected Arrays.

To Modify Multiple Rows

Use this procedure to quickly configure multiple radios to have the same settings.

1. **Step 1 - Select Arrays:** For each Array whose radios you wish to modify, select the checkbox at the beginning of the row. To select all rows, click the checkbox in the header row. Click again to deselect all rows.

Click **Next>** when the desired rows are selected.

2. **Step 2 - Edit Radio Settings:** Select the radios to be edited by clicking their check boxes. Then click **Bulk Edit**. This displays blank fields for all of the settings that are modifiable in bulk: **Enabled**, **Band**, **Bond Mode**, **Tx dBm**, **Antenna**, **Channel**, **Cell Size**, **Rx dBm**, and **Locked**. (Figure 292)

Xirrus Management System

Select the changes you would like to make to all selected radios and click OK.

Enabled: ☒ Unchanged ☐ Yes ☐ No

Band: 5 GHz

Bond Mode: monitor

Antenna: 5 GHz

Channel:

Cell Size:

Tx dBm:

Rx dBm:

Locked: ☒ Unchanged ☐ Yes ☐ No

OK Cancel

Figure 292. Bulk Configuration (Radio Settings)

Click **OK** when done. The Bulk Edit dialog closes, and your desired changes will be displayed in the radio settings table. Note that the new

values have not yet been sent to the Arrays. Take a moment to review your changes. You may individually edit any incorrect settings.

Click **Finish** when satisfied with the changes.

3. **Step 3 - View Results:** The web client will apply the changes you entered, and display the success or failure of the configuration operation on the selected radios.

To Export Radio Settings

This option exports channel and other radio settings on selected Arrays to an Excel file or to a CSV file—a set of comma-separated values that are compatible with Microsoft Excel. This file is useful in a number of ways:

- As a backup of the current configuration, especially since the settings in the file may be imported to restore this configuration.
- To provide Xirrus Customer Support with a snapshot of the configuration of your network, at their request.
- You may edit the settings in this file and then import the changed values. Take care only to modify the fields that are editable on the Bulk Configuration page.

This feature is used in exactly the same way as the export feature for network settings. Please see [“To Export Network Settings” on page 461](#) for instructions. To import a file that was exported from the Radio Settings page, see [“To Import Radio Settings” on page 469](#).

Note that any time you click the **Export** button or use the **Export Settings** link, the old unedited values will be exported, unless you have completed saving your edited values to the Arrays.

To Import Radio Settings

This option allows you to change settings on radios by importing a file that was exported from the Radio Settings page. (See [“To Export Radio Settings” on page 469](#) for details). This feature is used in exactly the same way as the import feature for network settings. Please see [“To Import Network Settings” on page 464](#) for instructions.

Advanced Config

The Advanced Config pages allow you to apply a file containing a complete or partial configuration to an Array. Using Advanced Config is described in the following topics:

- “About Advanced Config Files” on page 470
- “Advanced Config Page” on page 471
- “Load from Array” on page 473
- “Deploy Configuration” on page 474

About Advanced Config Files

A Config File is a set of CLI commands to configure an Array. It may consist of:

- a complete set of commands to define every setting on the Array,
- an almost complete set that just omits a few items, like leaving out the IP address commands in order to leave the Array address as is,
- or a partial set of commands that just deal with particular aspects of the Array’s configuration.

The file may be copied from the existing configuration of an Array that you select as a model, or may be entirely typed in. For example, if Xirrus Customer Support sends you a config file, you may copy that file and paste it in to the config file editor to create your file.



*This feature is intended for **advanced users** who are familiar with use of the Xirrus Wi-Fi Array CLI and configuration files. Only **expert users** should use the option to create the entire configuration file.*

If you start with a config file copied from the existing configuration of an Array, you may edit the file to contain only the settings that you wish to copy to other Arrays. The file makes incremental changes to the settings on an Array when it is deployed. Thus, **settings not defined in the config file will be left unchanged.**

Config files are useful in a number of situations. In particular, they are the *only* way to apply new features to Arrays before those features have been incorporated in XMS.

Advanced Config Page

Use this page to type in the entire config file from beginning to end (i.e., “from scratch”), to modify an existing file, and to manage your config files. Only expert users should create a config file from scratch. As an alternative, we strongly recommend that you use the [Load from Array](#) page to download a config file from an Array. It may then be managed with this page.

Open this configuration page by clicking the **Configure** button near the top of the window, then select **Advanced Config** on the left.

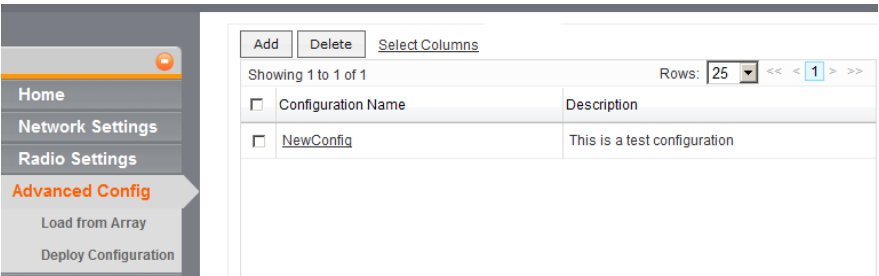


Figure 293. Advanced Config Page

To create a config file from beginning to end (“from scratch”)

This procedure opens the config file editor so that you can type in the CLI command lines of the config file, or cut and paste commands from an existing config file into the editor.

Click the **Add** button on the upper left of the **Advanced Config** page. The config file editor appears. (Figure 294)

Enter **Configuration Name**, a name for this config file. Then enter an optional **Description**. You may type, paste text, or edit your commands in the large gray box at the bottom of the page. It is especially useful to copy large sections of text from a configuration file that has been quality-tested elsewhere, and paste the text into the editor box.

Editing the Configuration File

You may type text to enter it in the box, and use the **Backspace** and **Delete** keys. You may use common selection and cut and paste keys:

- Ctrl+a: select all
- Ctrl+c: copy selected text
- Ctrl+x: cut selected text
- Ctrl+v: paste text (may be from an application other than XMS)
- Shift+Click: select contiguous text up to clicked location
- Shift+Arrow: select contiguous text in direction of arrow
- Use your browser's search functions if you want to search for text

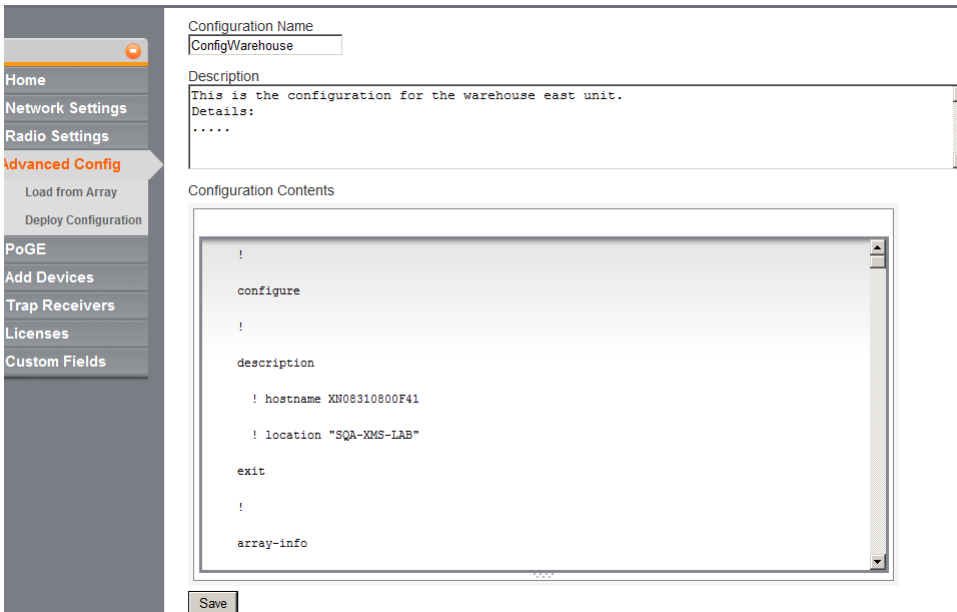


Figure 294. Advanced Config Editor

Click **Save** when done. The editor closes, and your new file appears in the list of config files. (Figure 293) Each **Configuration Name** in this list is a link. To edit a file, simply click the link. If you wish to remove a config file, select the checkbox to the left of it and click the **Delete** button.

Load from Array

Use this page to download the configuration of a model Array to a config file. This method of creating a config file is highly recommended for most users. Only *expert* users should type in the entire file as described in “[Advanced Config Page](#)” on page 471!

Start by clicking the **Configure** button near the top of the window, then select **Advanced Config** on the left. When the **Load from Array** link appears underneath, click it.

The web client displays a list of the Arrays in the XMS database. Select the checkbox to the left of the “model” Array in the list, then click **Next**. The web client displays a **Loading** message while the download proceeds.

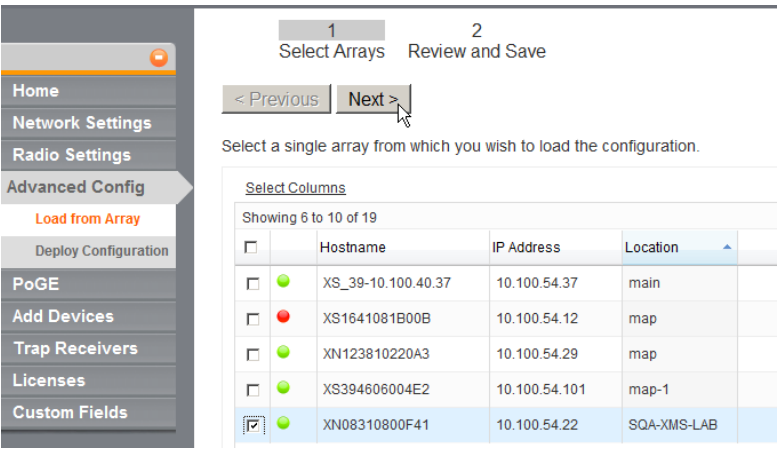


Figure 295. Load from Array

When the download is complete, you are returned to the [Advanced Config Page](#) and the new file appears on the list of config files. The new file’s name is the same as the host name of the Array from which it was downloaded. You may edit this file in the usual way, as described in “[Advanced Config Page](#)” on page 471.

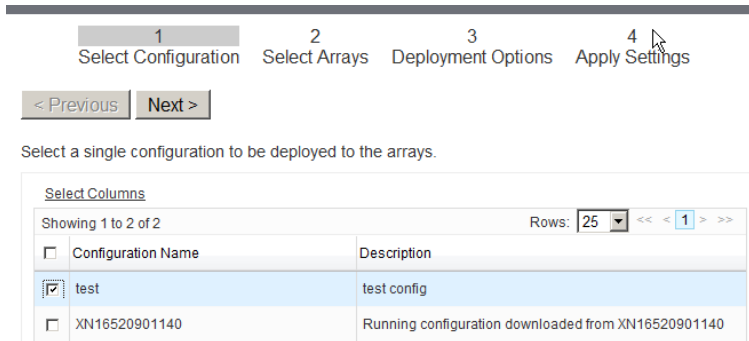
When you download a config file from an Array, the file represents the entire configuration of the Array, except that XMS makes certain modifications to the file for your convenience:

- CLI commands are added to reset all the IAPs and then bring them back up. Similarly, other settings such as SSID, User Group, DHCP Server, and VLAN will be reset and brought back up. This guarantees that when the config file is deployed to another Array, all of these settings will be applied to an Array starting from a known baseline, due to the resets.
- All other radio (IAP) settings are commented out, so that no radio settings will change. Certain other settings, such as Host Name, Location, and ArrayOS primary and backup software images will be commented out as well in order to prevent these device-specific settings from being applied to multiple Arrays.

Deploy Configuration

Use this page to apply one of the advanced config files that you have already created to one or more Arrays.

Start by clicking the **Configure** button near the top of the window, then select **Advanced Config** on the left. When the **Deploy Configuration** link appears underneath, click it. The web client displays a list of the available config files. (Figure 296)



1 2 3 4

Select Configuration Select Arrays Deployment Options Apply Settings

< Previous Next >

Select a single configuration to be deployed to the arrays.

Configuration Name	Description
<input checked="" type="checkbox"/> test	test config
<input type="checkbox"/> XN16520901140	Running configuration downloaded from XN16520901140

Figure 296. Select Advanced Config File to Deploy

Select the checkbox to the left of the desired config file in the list, then click **Next**. The web client displays a list of the Arrays in the XMS database. (Figure 297)

1

2

3

4

Select Configuration Select Arrays Deployment Options Apply Settings

< Previous

Next >

Cancel

Select the arrays to which you wish to deploy the configuration.

Select Columns

Showing 1 to 2 of 2

Rows: 25 << < 1 > >>

<input type="checkbox"/>	Hostname	IP Address	Location	
<input checked="" type="checkbox"/>	XN16520901140	10.100.54.26	XMS-map	
<input type="checkbox"/>	XS08010800E36	10.100.56.31	VLAN_racks	

Figure 297. Select Arrays for Deployment

Select the checkbox to one or more Arrays in the list to which the config file is to be deployed, then click **Next**. The web client displays deployment options. (Figure 298)

1

2

3

4

Select Configuration Select Arrays Deployment Options Apply Settings

< Previous

Deploy >

Cancel

Select deployment options.

☒ Permanently save this configuration on the array

Figure 298. Select Deployment Options

Select the checkbox to **Permanently save this configuration on the Array**. If you do not check this box, the commands in the config file will be deployed on the selected Arrays, but they will not be saved. Thus, they will not be reapplied if you reboot the Array. Click **Deploy** to apply the config file to the selected Arrays. The web client displays deployment results. (Figure 299)

1 2 3 4
Select Configuration Select Arrays Deployment Options Apply Settings

< Previous
Finish
Cancel

[Select Columns](#)
[Export](#)

Showing 1 to 1 of 1
Rows: 25 << 1 >>

	Message	Hostname
●	Done deploying configuration	XN16520901140

Figure 299. Select Deployment Options

The **Message** list indicates when the deployment is in progress for each of the selected Arrays, and then shows whether the deployment has been completed.

PoGE

This page shows the Power over Gigabit Ethernet (PoGE) injectors in your Xirrus network. (Only the PoGE models that have remote management capability are listed on this page.) The PoE page provides tools for associating each PoGE injector port with the Array port to which it is physically connected. You may then use XMS to monitor the status of injectors and to power down or power-cycle Arrays by controlling the injector ports that drive them.

The **PoGE** page shows all injector ports and indicates if ports are free or shows the Array ports to which they are connected. On the left of the window, an **Arrays** link appears which lists all Array gigabit ports and shows whether they are already connected to an injector port or are free.



The PoE page is used to associate Array ports with injector ports so that the XMS database reflects the physical connections powering Arrays in your network. You must specify these connections explicitly in XMS—they are not discovered automatically.

For complete details on the use of the Injectors and Arrays pages, and on discovering and managing PoGE injectors with XMS, please see **“PoGE Injectors” on page 211**.

Add Devices

Use the Add Devices configuration pages to enter all the settings necessary to have XMS find the Arrays on your Wi-Fi network and add them to its database of managed devices. You can enter SNMP settings, add devices and networks, and enter Array SSH user information. For a detailed discussion of how XMS adds devices and how SNMP must be configured on Arrays and on XMS to support it, please see **“Discovering the Network” on page 67**.

To quickly start adding devices to XMS for your network, please see **Overview of Adding Devices** below.

Each of the Add Devices pages is separately discussed in the following topics:

- **“Add Devices” on page 480**
Adds a specific device, range of devices, or list of devices to XMS.
- **“SNMPv2 And SNMPv3 Settings” on page 482**
Adds or deletes SNMPv2 community names and SNMPv3 users.
- **“SSH Users” on page 485**
Add user accounts that XMS can use when it must log in to Arrays for some management functions.
- **“Add Networks” on page 486**
Adds a subnetwork for XMS to scan for Xirrus devices.

Note that in this chapter, the term *device* refers to a Xirrus Array or PoGE injector.



*To allow XMS to find a device (Array or PoGE injector), the device must have SNMP enabled and its community string must match one of the strings listed in the Discovery window. See **“SNMPv2 And SNMPv3 Settings” on page 482**. The default SNMPv2 community string in XMS matches the Array default value.*



When an Array boots up, it sends an SNMP trap to the XMS server's default hostname, *xirrus-xms*. XMS can then add it to its managed devices list. This Phone Home feature requires DNS to resolve the hostname *xirrus-xms* correctly. Thus, if you change the host name of the XMS server, you must configure DNS to resolve *xirrus-xms* to the actual name of the XMS server host.

Overview of Adding Devices

This section provides a quick summary of the steps required to start adding devices to XMS. For complete details on this process, please see the discussions in [Discovering the Network](#).

Once started, this process uses SNMP to automatically find Xirrus Arrays and PoGE injectors in the subnets that you specify. ([Figure 300](#)) No networks are discovered by default, so you must add the subnets containing your Arrays.

1. In the web client, click **Configure** on the top and then click **Add Devices** on the left.
2. To add **SNMPv2 Community Names** or **SNMPv3 Users** to match the strings being used by your Arrays, click **SNMPv2 Settings** or **SNMPv3 Users**. For XMS to discover and manage a device, the device must have SNMP v2 and/or v3 enabled. The device's SNMPv2 community string or SNMPv3 read-write authentication settings must match one of those defined here for discovery.

The default SNMPv2 community name (**xirrus**) allows XMS to discover new Arrays that still have default SNMP settings (SNMPv2 is enabled with its **Read Write Community String** set to **xirrus**). Also, each Array's **Trap Host 1 IP Address** is set to the hostname **Xirrus-XMS** by default (for the [Phone Home](#) feature).

Enter the appropriate SNMP settings. For more details, see [“SNMPv2 And SNMPv3 Settings” on page 482](#).

3. To add networks where XMS should search for devices, click the **Add Networks** link on the left. (Figure 300) When the page appears, click the **Add Network** button on the upper left. In the **Add New Network** dialog box, enter the subnet's **Network Address** and **Subnet Mask**. Select **Start Discovery** so that the discovery process will be initiated, then click **OK**. Note that the newly entered network is displayed in the list of networks for discovery.

Discovery begins soon after adding a network. Be careful to specify the subnet accurately, to avoid creating excess traffic by discovering a needlessly large network.

To add individual Arrays or power supplies, use the **Add Devices** link on the left instead.

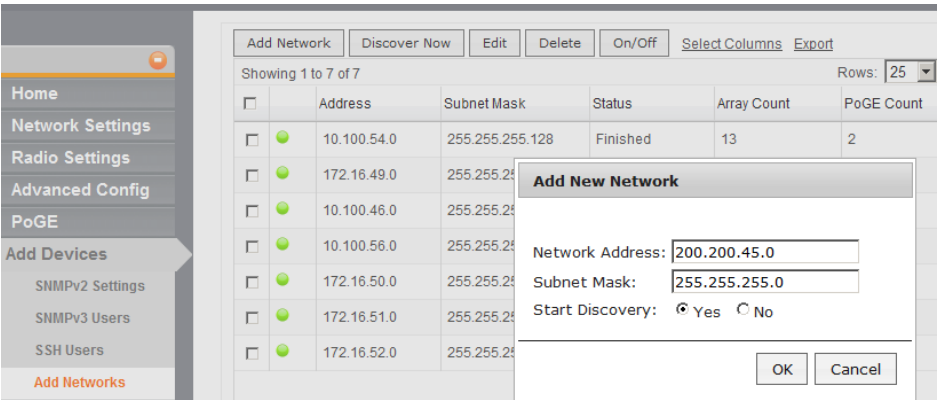


Figure 300. Managing Discovery of Devices

Add Devices

This page is used to manually add one or more Arrays and/or PoGE power supplies to XMS, rather than specifying a network and having XMS discover them. You may enter a single device IP address, a range of addresses, or a list of addresses. This last option is especially useful if you have an Excel spreadsheet with a list of Arrays and their addresses. Simply copy and paste the single column that has the device IP addresses.

Open this configuration page by clicking the **Configure** button near the top of the window, then select **Add Devices** on the left.

Select whether to add a **Single Device**, an **IP Range**, or **Multiple Devices** by clicking the appropriate tab.

- **Single Device (Figure 301)**

Enter the **IP Address** of the single device to be added to XMS. Click the **Discover** button.

1 Enter Device IP Addresses 2 Review

< Previous Discover >

Enter the IP address of the device you wish to discover.

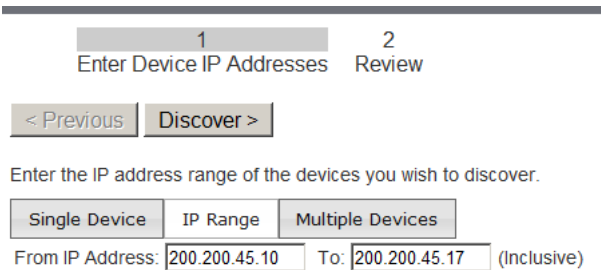
Single Device IP Range Multiple Devices

IP Address:

Figure 301. Discover a Single Device

● **IP Range (Figure 302)**

Enter the start of the range in the **From IP Address** field. Enter the end of the range in the **To** field. XMS will check every address in the range, up to and including the **To** address. Click the **Discover** button. At each address, if it finds an Array or management-capable Xirrus PoGE power supply, XMS will add the device to its list of discovered devices.

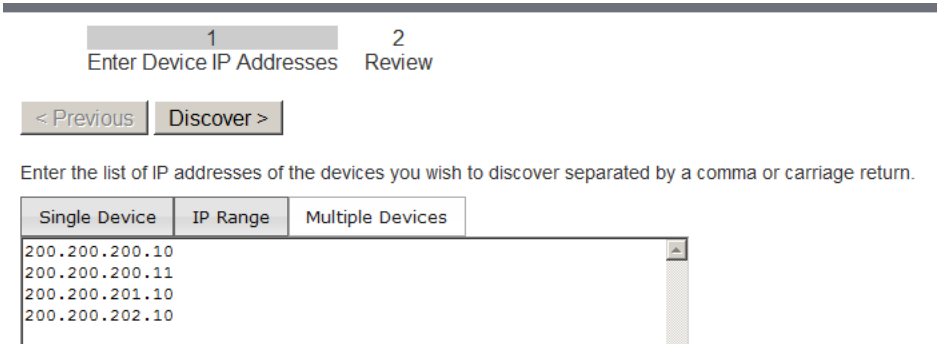


The screenshot shows a web interface for discovering devices. At the top, there are two tabs: '1 Enter Device IP Addresses' and '2 Review'. Below the tabs are two buttons: '< Previous' and 'Discover >'. A text prompt says 'Enter the IP address range of the devices you wish to discover.' Below this are three tabs: 'Single Device', 'IP Range' (which is selected), and 'Multiple Devices'. Under the 'IP Range' tab, there are two input fields: 'From IP Address:' with the value '200.200.45.10' and 'To:' with the value '200.200.45.17'. To the right of these fields is the text '(Inclusive)'.

Figure 302. Discover a Range of IP Addresses

● **Multiple Devices (Figure 303)**

Type or paste a list of as many IP addresses as you like in the box, separated by commas, spaces, or carriage returns. You may paste a list of IP addresses obtained from an Excel .csv (comma-separated values) file. Click the **Discover** button. XMS will check every address in the list. At each address, if it finds an Array or management-capable Xirrus PoGE power supply, XMS will add the device to its list of discovered devices.



The screenshot shows a web interface for discovering devices. At the top, there are two tabs: '1 Enter Device IP Addresses' and '2 Review'. Below the tabs are two buttons: '< Previous' and 'Discover >'. A text prompt says 'Enter the list of IP addresses of the devices you wish to discover separated by a comma or carriage return.' Below this are three tabs: 'Single Device', 'IP Range', and 'Multiple Devices' (which is selected). Under the 'Multiple Devices' tab, there is a large text area containing a list of IP addresses: '200.200.200.10', '200.200.200.11', '200.200.201.10', and '200.200.202.10'. A vertical scrollbar is visible on the right side of the text area.

Figure 303. Discover a List of IP Addresses

After you click the **Discover** button, XMS will attempt to discover a Xirrus Array or managed power supply at all of the IP addresses that you entered. It will display the results of discovery, listing whether it succeeded or failed at each address. **(Figure 304)** If discovery fails at an address, XMS will still try all the rest of the addresses that you entered. Note that if you enter a device that is already in the XMS database, XMS will attempt to “refresh” the device by obtaining up-to-date information about it.

You may use the **Cancel** button if you wish to abort discovery while still in progress. This will stop XMS from finding any additional devices, but will not remove any devices that have just been discovered.

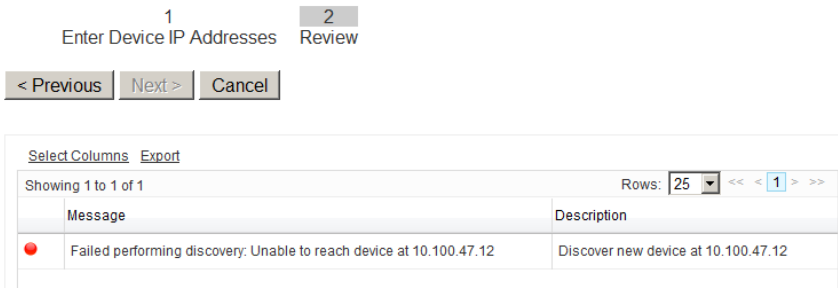


Figure 304. Review Results of Adding Devices

SNMPv2 And SNMPv3 Settings



*For a device to successfully **Phone Home** (announce its presence to XMS) or be discovered, SNMPv2 or SNMPv3 must be enabled on the device. For SNMPv2, the read-write community string (i.e., community name) must match one of the strings listed in the Discovery window. For SNMPv3, the Array’s read-write user name and passwords must match one of the entries listed in the Discovery window.*

These pages are used to add or delete SNMPv2 community names and SNMPv3 users.

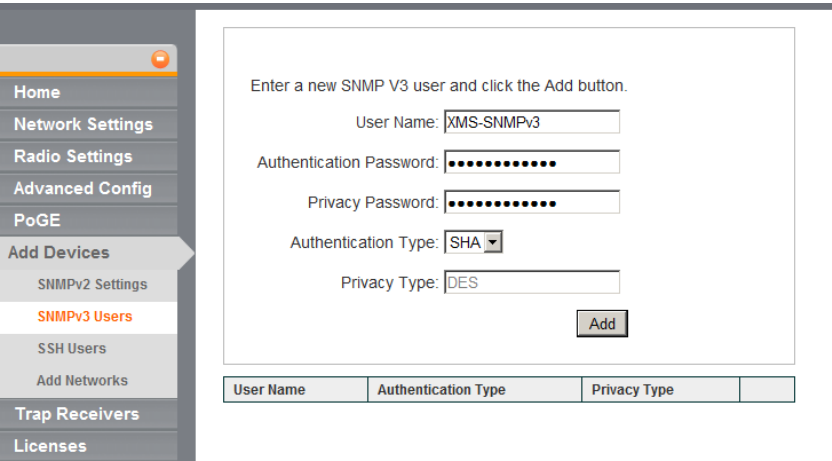
The XMS discovery process searches networks using both SNMPv2 and SNMPv3. Since SNMPv3 offers much improved security, this version is preferred by XMS.

Discovery will search for devices using SNMPv3 first. When an Array is discovered using SNMPv3, then XMS uses that version for communication with the Array from then on. When an Array or PoGE injector is discovered via SNMPv2, then XMS uses SNMPv2 to communicate with the device. Injectors support SNMPv2 only.

XMS discovery has default SNMPv2 entries which match the factory default SNMP v2 settings in Arrays and PoGE injectors. However, for proper security on your Xirrus devices, we **STRONGLY** recommend that you change these defaults on Xirrus devices by entering your own SNMPv3 user names and passwords and/or SNMPv2 community strings. Thus, you must add those community names or user names/passwords to XMS for discovery to find those devices.

*NOTE: Although XMS does not have any SNMPv3 usernames or passwords defined by default, Xirrus Arrays do have default entries. The Array's default read-write username and password are **xirrus-rw**; the default read-only username and password are **xirrus-ro**.*

To add an **SNMPv3 User**, click the **Configure** button near the top of the window, then select **Add Devices** on the left. Click the **SNMPv3 Users** link on the left when it appears. (Figure 305)



The screenshot shows the XMS web client interface. On the left is a navigation menu with the following items: Home, Network Settings, Radio Settings, Advanced Config, PoGE, Add Devices (highlighted), SNMPv2 Settings, **SNMPv3 Users** (highlighted in orange), SSH Users, Add Networks, Trap Receivers, and Licenses. The main content area displays a form titled 'Enter a new SNMP V3 user and click the Add button.' with the following fields: 'User Name' (containing 'XMS-SNMPv3'), 'Authentication Password' (masked with dots), 'Privacy Password' (masked with dots), 'Authentication Type' (a dropdown menu showing 'SHA'), and 'Privacy Type' (a dropdown menu showing 'DES'). An 'Add' button is located at the bottom right of the form. Below the form is a table with the following structure:


User Name	Authentication Type	Privacy Type	
-----------	---------------------	--------------	--

Figure 305. SNMPv3 Users

Enter the new **User Name** and **Authentication** and **Privacy Passwords**. Set the **Authentication Type** to match your Arrays. Leave the **Privacy Type** set to **DES**. Click **Add** when done. The new User account will be added to the list, located under the dialog box.

To add an **SNMPv2 Community Name**, click the **Configure** button near the top of the window, then select **Add Devices** on the left. Click the **SNMPv2 Settings** link on the left when it appears. (Figure 306)

Enter the new **Community Name** and click **Add**. The new **Community Name** will be added to the list, located under the dialog box.



Enter a new community name and click the Add button.

Community Name:

Add

Community Name	
omar	Delete

Figure 306. SNMPv2 Settings

The next time that the discovery process runs after adding a new SNMP v2 or v3 entry, XMS will use all of the Community Names or Users listed. Adding or deleting a name on a list will not trigger discovery to run immediately. The new name will be used by the next discovery process (but will not be used now, if discovery is currently running). To trigger a discovery process using the new entry, use the Discover Now button described in [“Add Networks” on page 486](#).

To delete an entry from either list, click the **Delete** button to its right. You will be asked to confirm the deletion. The next time that the discovery process runs, it will use the Community and User Names listed at that time. Note that discovery will not remove devices from its device list if they have a community or user name that was deleted. Once a device is discovered, it stays on the device list even

if you remove the community or user name or disable discovery. The device remains until you delete it manually.

SSH Users

Some policies, such as **Software Update** and **Web Page Redirect (WPR)**, and **Advanced Config**, require Arrays to download files. When it instructs an Array to fetch a file from the server, XMS must log in to the Array shell. Depending on the configuration of the Array, authentication may use the Array's local accounts or may use a RADIUS server. In either case, the XMS server needs to know a **Username** and **Password** to gain access to the Array shell.

To define this Array login information, use the **SSH Users** page. Click the **Configure** button near the top of the window, then select **Add Devices** on the left. Click the **SSH Users** link on the left when it appears. (**Figure 307**)

Enter an Array's **User Name** and **Password**, and click **Add**. The new entry will appear in the Array Shell Authentication list, located under the dialog box. You may use the **Delete** button to remove a selected entry, if necessary.

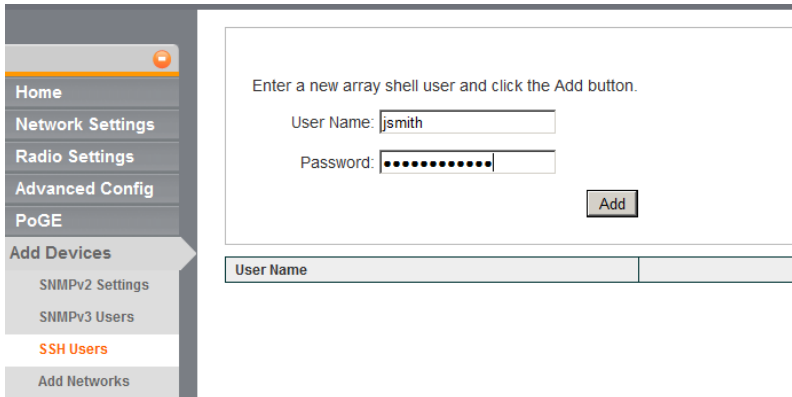


Figure 307. Adding SSH Users

These authentication entries are not used by the discovery process itself, but are managed on this window for convenience. When XMS needs to log in to an Array's shell, it tries entries from the list until it finds one that works. Then it will

remember to use this login for this Array. On future login attempts to the same Array, it will try the remembered login first.

Add Networks

To add networks for discovery, click the **Configure** button near the top of the window, then select **Add Devices** on the left. Click the **Add Networks** link on the left when it appears. (Figure 308) When the page appears, click the **Add Network** button on the upper left. In the **Add New Network** dialog box, enter the subnet's **Network Address** and **Subnet Mask**. Select **Start Discovery** so that the discovery process will be initiated, then click **OK**. The newly entered network will be displayed in the list of networks for discovery.

Discovery begins soon after adding a network. Be careful to specify the subnet accurately, to avoid creating excess traffic by discovering a needlessly large network.

To add individual Arrays or power supplies for discovery, use the **Add Devices** link on the left instead.

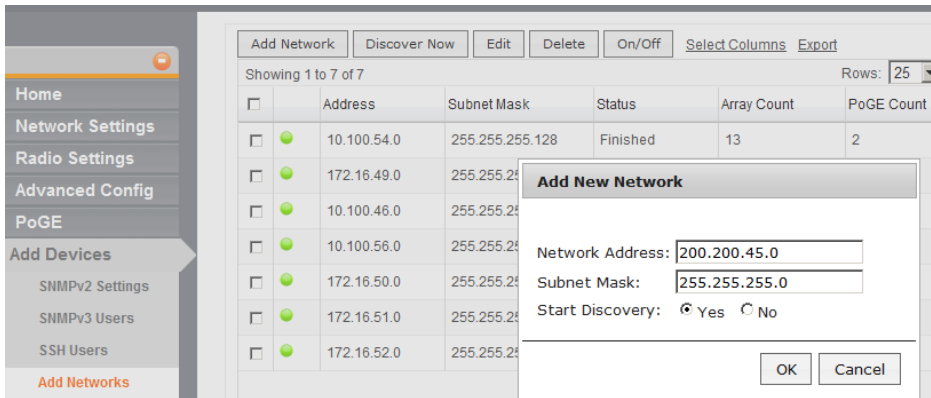


Figure 308. Add Networks for Discovery

The list of networks for discovery shows the following information.

- **Address**—the **Network Address** that you entered. The icon to the left of the address is green if you enabled **Start Discovery**, and yellow if you

have disabled discovery for this network. Note that you may use the Edit button to toggle **Start Discovery**.

- **Subnet Mask**—the mask that you entered.
- **Status**—the status of the discovery process. The status may be **Finished** (discovery complete), **Disabled** (Start Discovery not enabled for this network), or **Discovering** (discovery is still in progress for this network).
- **Array Count**—the number of Arrays discovered on this network so far.
- **PoGE Count**—the number of PoGE power injectors discovered on this network so far.

The toolbar above the list of networks provides a number of additional functions:

- **Discover Now**—click this button to start discovery immediately. This will start discovery on the selected networks only.
- **Edit**—to change a network (**Network Address**, **Subnet Mask**, and whether **Start Discovery** is enabled), select the network and click **Edit**.
- **Delete**—to remove networks, select the desired networks and click **Delete**. You will be asked to confirm the deletion.
- **On/Off**—this button toggles whether **Start Discovery** is enabled on the selected networks. If you use this button to enable **Start Discovery**, then the discovery process will be started immediately on the selected networks.

Note that discovery will not remove devices from the XMS database if you delete their network, if they are on a network where discovery has been disabled, or if you have edited the IP address so that their original network is no longer listed for discovery. Devices remain on the list until you delete them manually.

Trap Receivers

Just as Arrays send SNMP traps to the XMS server, the XMS server can send traps to top-level supervisory software. Any Array event that gets escalated to an alarm will be forwarded to the trap receivers that you set up. The receiver for these traps might be a Manager of Managers (MOM) or an application like HP OpenView running at the NOC. Use the **Trap Receivers** page to set up one or more destinations for these traps.

Destination Host	Destination Port	Community Name	Description	Enabled	
10.100.54.41	162	xirus		<input checked="" type="checkbox"/>	Remove

Figure 309. Trap Receivers

To add trap receivers, click the **Configure** button near the top of the window, then click **Trap Receivers** on the left. (Figure 309) Enter the **Host Name or IP Address** of the destination that is to receive traps sent by the XMS server. If needed, change the **Port Number** from its default value of 162. Set the **Community Name** needed for access to this destination. Add a **Description** for this receiver if desired, and set **Enabled** to make this entry active. Click **Add** when done. The new entry will be displayed in the list of trap receivers.

If necessary, you may use the **Remove** button to the right of an entry to remove this trap receiver from the list.

Array Licenses

This page displays and manages the licenses for Arrays in your Xirrus network. You may view the license of each Array and deploy new or upgraded licenses.

For complete details on the use of this page, please see [“Managing Array Licenses” on page 189](#).

Custom Fields

The Custom Fields pages allow you to define your own custom columns and action buttons for the **Monitor—Arrays** table and the **Configure—Home Page**. These fields allow you to add all kinds of information and functionality to XMS for Arrays. For example, you might use extra columns to add an Asset Tag to each Array, or to add notes on support cases.

Using a Custom Action, you might add a button to access your company’s web portal for managing assets. Then you can open the portal to manage a selected Array with a click of the button.

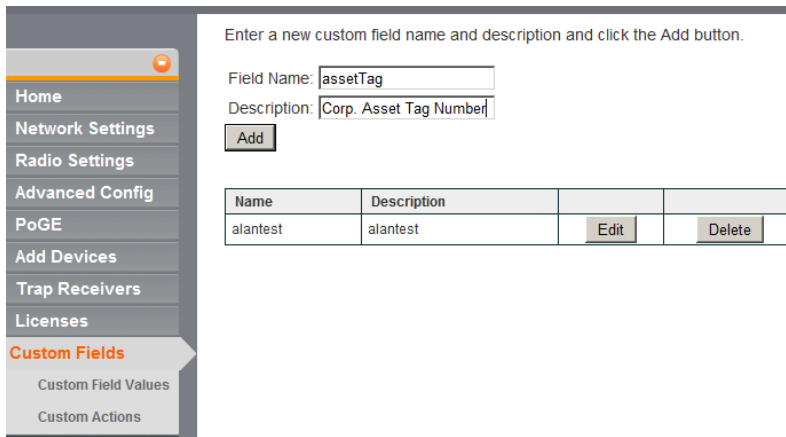
This feature is discussed in the following pages:

- **Custom Fields Page**
Use this page to define a new column to add to the Arrays table, where you can place Array information that your company uses.
- **Custom Field Values**
Use this page to place data in the new column that you created above.
- **Custom Actions**
Use this page to add a button for a new function. Define the action that the button will take by specifying a URL. The URL can start your desired web application with data based on the currently selected Array.

Custom Fields Page

This page is used to define a new column for the Arrays list. This column will be available on the **Monitor—Arrays** page and the **Configure—Home Page**. You may add up to five new columns and use them for any sort of information that you'd like to keep with each Array. For example, you might add an asset tag column, or a column for notes regarding support actions for this Array.

Open this configuration page by clicking the **Configure** button near the top of the window, then select **Custom Fields** on the left.



Enter a new custom field name and description and click the Add button.

Field Name:

Description:

Name	Description		
alantest	alantest	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

Figure 310. Custom Fields Page

Enter the desired **Field Name** for the new column (this name will be used as the header for this column in the Arrays list), and add an optional **Description** for your reference if you wish. The description will only appear in the list of fields on the Custom Fields page—it is not used anywhere else. Click **Add** when done. You may repeat the procedure to create up to a total of five new fields. Each new column may be used to contain strings up to 255 characters long.

The new field will be displayed in the list below the **Add** button. You may remove an entry by clicking the **Delete** button to its right. You may modify the **Field Name** or **Description** by clicking the **Edit** button to its right. If you have populated this custom column with data, the data will be unaffected and will still exist under the edited **Field Name**.

The new column is not automatically displayed on the Arrays list. To display it, go to the **Monitor—Arrays** page or the **Configure—Home Page** and use the **Select Columns** function. The new field is typically found by scrolling to the bottom of the **Hidden Columns** list. See “**Select Columns**” on page 442 for more details.

Continue to the next section, **Custom Field Values**, to populate the new column with data for as many Arrays as you like.

Custom Field Values

This page populates your new column (created with the **Custom Fields Page**) with data values. There is also a **Bulk Edit** option that allows you to enter identical data for multiple Arrays in one step, in the same way that you can use Bulk Edit for the **Network Settings** and **Radio Settings** pages.

Open this configuration page by clicking the **Configure** button near the top of the window, then select **Custom Fields** on the left. Click the **Custom Field Values** link when it appears on the left.

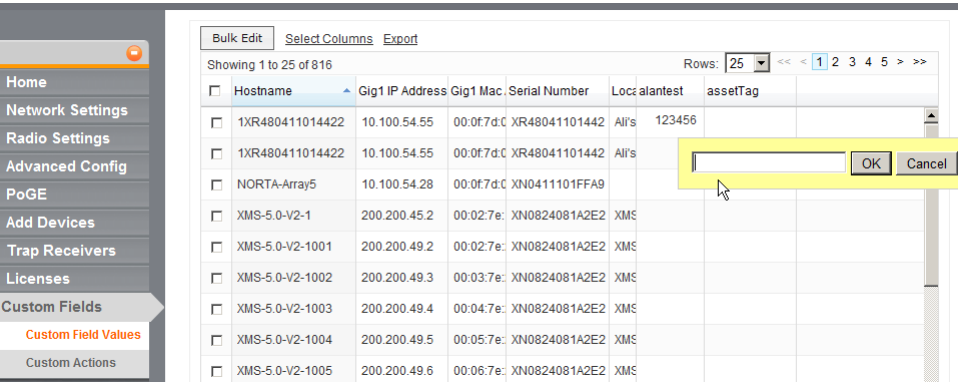


Figure 311. Custom Field Values—Adding a single value

Before you add values, you must make sure that the desired custom column is displayed. If you have scrolled all the way to the right of the Arrays list and the new column is not visible, the use the **Select Columns** link to add it to your display. You may also wish to change the custom column’s position to be further to the left. See “**Select Columns**” on page 442 if you need more details. Note that

you can also change the new column's position by simply dragging its column header in the Array list (see [“Rearranging and Resizing Columns in a Table” on page 443](#)).

To enter a value for an individual Array, simply click its entry in the custom column. ([Figure 311](#)) A dialog box is displayed where you can type the desired string, up to 255 characters long. Click **OK** when done to save the value, or click **Cancel** to abort.

Use **Bulk Edit** to quickly configure multiple Arrays to have the same value. Select the checkbox at the beginning of each row that is to contain this value. To select all rows, click the checkbox in the header row. Click again to deselect all rows.

Click **Bulk Edit** when the desired rows are selected. The Bulk Edit Custom Field Values dialog box appears. Enter the desired string, up to 255 characters, and click **OK**. ([Figure 312](#))

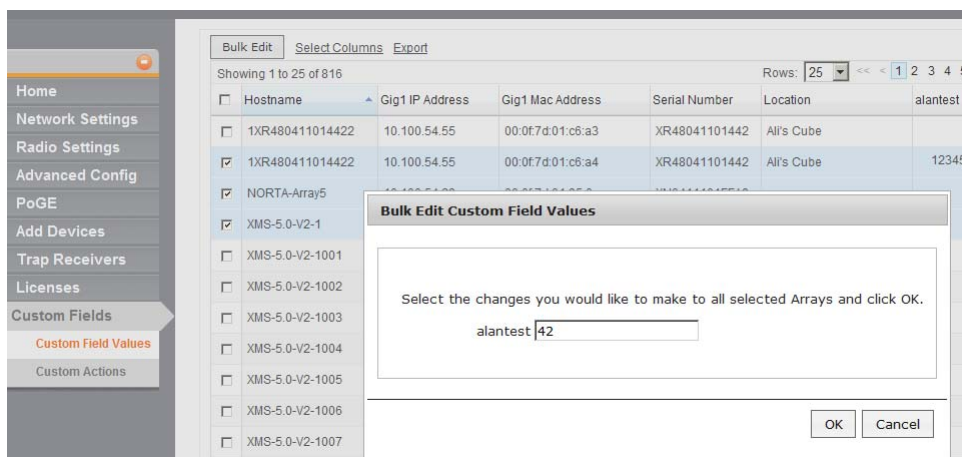


Figure 312. Bulk Configuration (Custom Field Values)

The value that you entered will be displayed in the Arrays list for the selected Arrays.

Custom Actions

This page allows you to define a custom button that adds a new function to the Arrays list. Associate an action with the button by specifying a URL to open when the button is pushed. The URL can include variables. For example, suppose you added the new column titled **assetTag** to the Arrays list using the **Custom Fields Page**, and then you entered values for this field for each Array using the **Custom Field Values** page. You could then define a new button labeled **Asset Tracking**, for example, that would go to your Asset Tracking Manager with a selected Array’s asset tag, using the URL:

```
http://track.xyzcorp.com/?assettagno=%assetTag%
```

You may choose to add the custom action button to the Monitor—**Arrays** page and/or to the **Configure—Home Page**. You may add a number of new custom actions.

Open this configuration page by clicking the **Configure** button near the top of the window, then select **Custom Fields** on the left. Click the **Custom Actions** link when it appears on the left.

Enter a new custom action and click the Add button.

Name

Description

URL (http or https)

Show in Monitor View ☐

Show in Configure View ☐

Add

Name	Description	URL	Show in Monitor	Show in Configure		
Xirus Support	Xirus Support Login	http://support.xirus.com	true	true	Edit	Delete
Asset Tracking	My Asset Tracking Program	http://track.xyzcorp.com/?assettagno=%assetTag%	true	true	Edit	Delete

Figure 313. Custom Actions Page

Enter the desired **Name** for the new button (this name will be used as the button’s label), and add an optional **Description** for your reference if you wish. The description will only appear in the list of entries on the Custom Actions page—it is not used anywhere else.

Enter the URL to go to when this custom button is pushed. The URL may include one or more variables:

`http://track.xyzcorp.com/?assettagno=%assetTag%`

You may use **http** or **https**. To pass a custom field name to a variable in the URL, just surround the name with % signs, as shown above for the custom field that we defined named **assetTag**.

XMS provides four predefined variables for your use:

- `%ipaddress%`
- `%hostname%`
- `%macaddress%`
- `%serialnumber%`

Select the page(s) where you want the new custom action button to appear. Select **Show in Monitor View** to add the custom action to the Monitor—[Arrays](#) page. Select **Show in Configure View** to add the custom action to the [Configure—Home Page](#). You may add the action to either, or to both.

Click **Add** when done.

The new custom action will be displayed in the list below the **Add** button. You may remove an entry by clicking the **Delete** button to its right. You may modify any of the actions settings by clicking the **Edit** button to its right.

XMS Administration

XMS may be administered from the XMS Java client and **The XMS Web Client**, and from a special tool provided with the server for Windows-based systems only: the Xirrus Server Management Tool (XSMT). The XMS Java client has tools for managing user accounts, changing the operating country, broadcasting a message to XMS users, and managing the database. The XMS web client and XSMT (for Windows-based servers) have tools for XMS server administration—both include advanced management operations.

The following sections describe simple administration tasks that are available from the XMS Java client:

- **“Country of Operation” on page 496**
- **“User Accounts” on page 497**
- **“Backup Manager” on page 499**
- **“Broadcast Message” on page 500**

An overview of managing the server is given in the following sections:

- **“About Managing the XMS Server” on page 501**
- **“About the XMS Database” on page 501**

Details of managing a Linux-based server are discussed in:

- **“Managing XMS on Linux-based Management Appliances” on page 502**

Details of managing a Windows-based server are discussed in:

- **“Managing XMS on Windows-based Systems” on page 523**

Country of Operation

The channels that are available for selection for an IAP will differ, depending on the country in which Arrays are used. To change the country of operation, select **Admin> Options** from the Java client's menu bar. Select the desired **Country** from the drop-down list and click **OK**. A message will be displayed to notify you that you must close your client and start it again. The default country is the United States.

The operating country will change the channels that are listed in “**IAP Setting Details (Figure 203)**” on page 311.



Figure 314. Country of Operation

User Accounts

From the **Admin** menu on the Java client's **Menu Bar**, select **User Accounts** to display the XMS User Accounts window. This window contains a list of all user accounts currently available, with tools to manage these accounts.

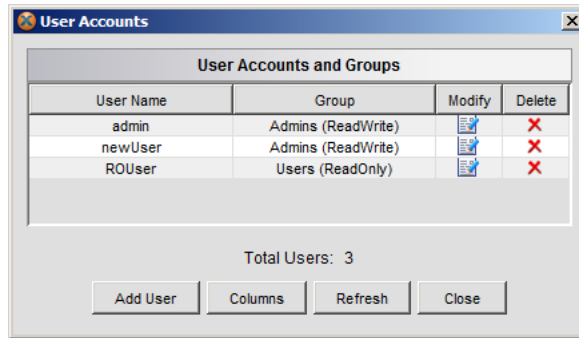


Figure 315. List of XMS User Accounts

The window also shows the configuration settings of each attribute listed in the window. **Figure 316** shows the Select Policy Attributes window for the XMS User Accounts—click the **Columns** button if you wish to display this window and change the fields displayed in the User Accounts window. For information about changing the attributes, go to **“Selecting the Columns Shown in a Policy Window”** on page 220.

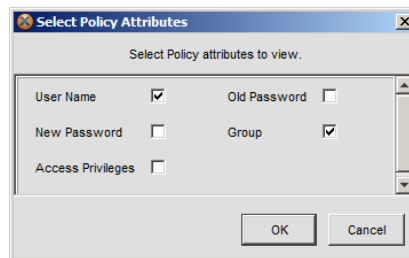


Figure 316. Select Policy Attributes (XMS User Accounts)

Creating a New User Account

An XMS User Account is created so that you can set up authentication criteria for users. To create a new user account, click on the **Add User** button in the XMS Java client's User Accounts window. The Manage User Accounts window is displayed.

Manage User Accounts

This window contains fields for assigning a user account, a user password, and user privileges.

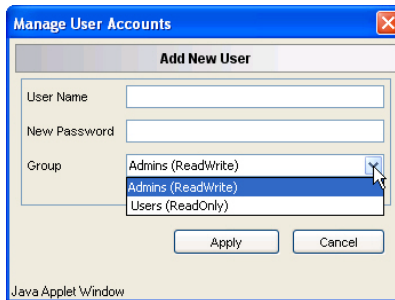


Figure 317. Manage User Accounts

- **User Name**
Enter a name for the new user.
- **New Password**
Enter a password for this user.
- **Group**
Choose the privilege level from the pull-down list, either **Admins** (Read/Write) or **Users** (Read Only).

Saving Your XMS User Account

When finished, click on the **Apply** button in the Manage User Accounts window to save the new account.

Backup Manager

This menu option allows you to schedule and manage backups of the XMS database from the XMS Java client. For more information about the database, please see **“About the XMS Database” on page 501**.

It is crucial to establish a backup schedule, since no default schedule exists on a newly installed XMS server.

From the **Admin** menu on the **Menu Bar** of the XMS client, select **Backup Manager** to display the Backup page in your browser. Backup management is identical, regardless of whether your XMS server is based on Linux or Microsoft Windows.

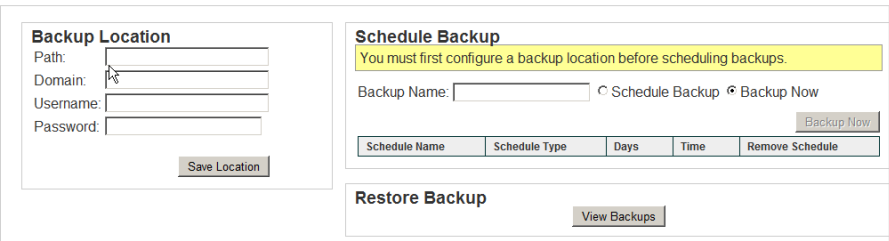


Figure 318. Database Backup Manager

This page has the same settings and is used in exactly the same way as the web client Backup page. See **“Web Client — Database Backup Settings” on page 511** for details.

Broadcast Message

Use this function to broadcast a message to XMS clients. For instance, you might use this message to warn users of a planned shutdown for maintenance. Select **Broadcast Message** from the Java client's **Admin** menu.

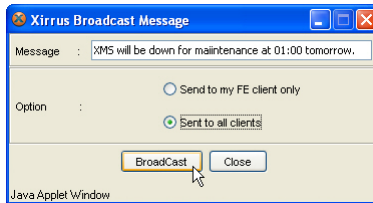


Figure 319. Broadcast Message

The Broadcast Message dialog box has the following fields.

- **Message**
Enter the text of the message to be sent to XMS clients.
- **Option**
Select whether you wish the message to be sent to all currently logged-in clients, or only to your own client. The second option is handy if you want to test using the broadcast feature.

Click the **Broadcast** button to send the message that you entered. The message is sent immediately to all clients, or just to your client, based on your selection.

About Managing the XMS Server

The tools for managing the XMS server are different, depending on whether the server is running on a Linux-based appliance or a Windows-based computer.

- Managing the XM-3320/XM-3340/XM-3360

These Linux-based Management Appliances use the browser-based XMS web client (**Figure 320 on page 502**) to manage the server. Database management functions are available in the web client, and may also be accessed by XMS Java client users.

See the sections starting with **“Managing XMS on Linux-based Management Appliances” on page 502.**

- Managing the XM-3300 and the XA-3330-CC

These Windows-based products use the Xirrus Server Management Tool (XSMT—**Figure 340 on page 526**) for advanced XMS server and database management. Many of the server’s settings are managed with the web client. Common database management functions are available in a browser-based **Backup Manager** that may be accessed by XMS Java or web client users.

See the sections starting with **“Managing XMS on Windows-based Systems” on page 523.**

About the XMS Database

The XMS database maintains the properties, status, and statistics for all the managed Wi-Fi Arrays represented in the network, as well as configured maps, policies, events and reports. It is important to back up your database regularly, which means establishing a schedule that suits your network’s activity.

***Note:** The XMS server does not have a default backup schedule, so it is **very important** for you to create a backup schedule after installation.*

You may set up a backup schedule to best suit your needs—the time required for a backup depends on the size of the database. And because XMS provides a client option for managing backups, they can be initiated from any client.

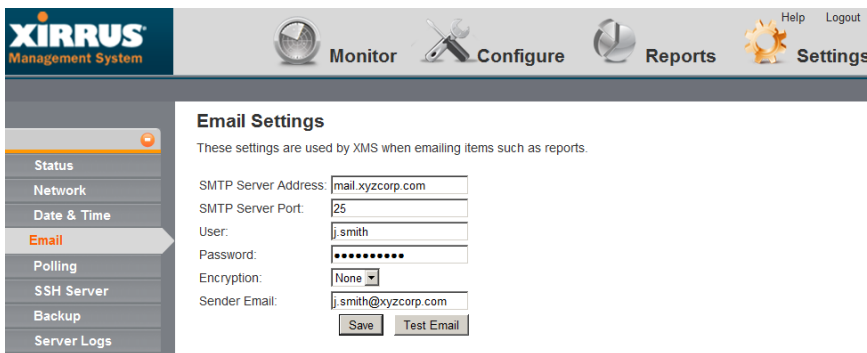
To manage the database, see:

- [“Backup Manager” on page 499](#)
- [“XSMT - Database Tools” on page 532.](#)

XMS does not purge old backups automatically. We recommend that you periodically review the backup files on your file server and delete older ones as needed, depending on the space available on the server.

Managing XMS on Linux-based Management Appliances

On the XM-3320/3340/3360, use the browser-based XMS web client ([Figure 320](#)) to perform mandatory initial configuration, to restart or reboot the server, and for server maintenance. The XMS server is started automatically when your Appliance is restarted.



The screenshot shows the XIRRUS Management System web client interface. The top navigation bar includes links for Monitor, Configure, Reports, and Settings. The left sidebar lists various system functions: Status, Network, Date & Time, Email (highlighted), Polling, SSH Server, Backup, and Server Logs. The main content area displays the 'Email Settings' page, which includes a description: 'These settings are used by XMS when emailing items such as reports.' The settings form contains the following fields: SMTP Server Address (mail.xyzcorp.com), SMTP Server Port (25), User (j.smith), Password (masked with dots), Encryption (None), and Sender Email (j.smith@xyzcorp.com). There are 'Save' and 'Test Email' buttons at the bottom of the form.

Figure 320. Server Management using the Web Client

The web client has multiple pages that manage settings for different XMS functions. Click a link on the left to go to the desired page. How to access the web client and descriptions of its pages are found in the following sections.

- [“Accessing the Web Client” on page 503](#)
- [“Initial Server Setup” on page 504](#)
- [“Web Client — Viewing XMS Server Status” on page 506](#)
- [“Web Client — Network Settings” on page 508](#)
- [“Web Client — Date and Time Settings” on page 509](#)

- “Web Client — Database Backup Settings” on page 511
- “Web Client — Polling Settings” on page 516
- “Web Client — Changing the SSH Server Address” on page 517
- “Web Client — Viewing Server Log Files” on page 518
- “Web Client — Performing Upgrades” on page 521
- “Web Client — Resetting the XMS Server” on page 522

Accessing the Web Client

Note: Web client access to the XMS server requires access to ports 9090 and 9443. Ensure that this port is open in any firewalls that exist between your browser and the XMS server.

To access the web client, set your browser’s URL to the XMS server machine’s IP address or host/domain name, followed by **:9090**. For example, **http://192.168.10.40:9090**. When the splash page appears, click **Web Client** on the lower right.



Figure 321. Starting the Web Client

Log in to the web client—the default for both fields is **admin**. In a few moments the web client Dashboard page appears. Click the **Settings** button at the top to display the Status page. (Figure 320) It shows a summary of the running state of the server. If you have not already performed the required initial setup for a

newly installed server, proceed to **Initial Server Setup**, below. Otherwise, you may skip that section.

*Note: You may use the Command Line Interface (CLI) to manage the XMS server. Access it at port 2022 and log in using **admin/admin**. Do **not** use port 22.*

Initial Server Setup

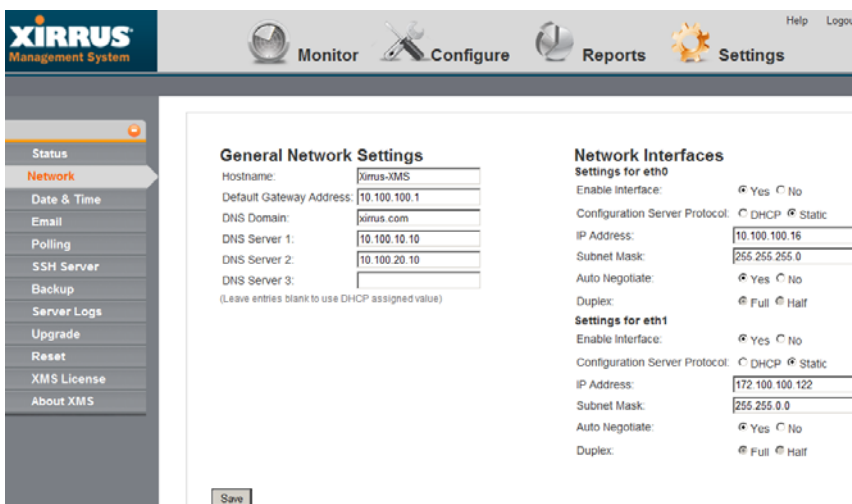
The following steps must be completed to configure the XMS server for proper performance. If you have already completed these steps, you may skip this section.

Initial Network Settings

See “**Web Client — Network Settings**” on page 508 for more information.

*Note: The XMS Server requires a valid license for full operation. If one is not present, it will be requested when you open a client. See “**Licensing the XMS Server**” on page 35.*

1. Select **Network** on the left to display the Network Settings window.



XIRRUS Management System

Monitor Configure Reports Settings

Status
Network
 Date & Time
 Email
 Polling
 SSH Server
 Backup
 Server Logs
 Upgrade
 Reset
 XMS License
 About XMS

General Network Settings

Hostname:
 Default Gateway Address:
 DNS Domain:
 DNS Server 1:
 DNS Server 2:
 DNS Server 3:
 (Leave entries blank to use DHCP assigned values)

Network Interfaces

Settings for eth0

Enable Interface: ☒ Yes ☐ No
 Configuration Server Protocol: ☐ DHCP ☒ Static
 IP Address:
 Subnet Mask:
 Auto Negotiate: ☒ Yes ☐ No
 Duplex: ☒ Full ☐ Half

Settings for eth1

Enable Interface: ☒ Yes ☐ No
 Configuration Server Protocol: ☐ DHCP ☒ Static
 IP Address:
 Subnet Mask:
 Auto Negotiate: ☒ Yes ☐ No
 Duplex: ☒ Full ☐ Half

Save

Figure 322. Changing Network Settings

Note: You may use one or both of the XMS Management Appliance's Ethernet ports. If using both, then one of the ports is typically reserved for management.

2. We recommend that you assign a Static IP address to each Ethernet port that is connected. The Appliance uses DHCP by default. If you have configured reserved leases for the ports in your DHCP server, skip to **Step 3** below. If you leave the DNS fields on this page blank and you are using DHCP, then the gateway and DNS servers configured in your DHCP server will be used.

If you have not assigned a reserved DHCP lease to the Appliance, select the **Static** option in **Configuration Server Protocol** under **Network Interfaces** for each Ethernet port that you are using. Make sure that **Enable Interface** is set to **Yes**, and enter the **IP Address** and **Subnet Mask**. Under **General Network Settings**, enter the **Default Gateway Address** and the **DNS Domain** and **DNS Servers**.

Note: The default IP address for eth0 is 10.0.2.10; for eth1 it is 10.0.2.11.

3. The **Hostname** of the Appliance is set to **Xirrus-XMS** by default. If you wish to change the Appliance's DNS Hostname, please see "**General Network Settings**" on page 508 for other changes that you should make to ensure proper operation of XMS in your network.

Initial Date/Time Settings

1. Click the **Date & Time** link on the left.
2. Select your **Time Zone**. Enable **Auto Adjust Daylight Savings** by clicking **Yes**.
3. We recommend that you leave **Use Network Time Protocol** enabled (this is the default). You may modify the **NTP Servers** (primary, secondary, tertiary), or leave them at the default values which use NTP Pool time servers (<http://www.pool.ntp.org/>).
4. If you disable **Use Network Time Protocol**, set the correct time and date in the appropriate fields.

Proceeding From Here

Create a backup schedule for the XMS database (“**Web Client — Database Backup Settings**” on page 511).

***IMPORTANT!** The XMS server does not have a default backup schedule, so you must create one after installation.*

Web Client — Viewing XMS Server Status

Click the **Status** link on the left to review the status and version number of the **XMS Server**, and the status and size of the **Database** (in bytes). The status of the **RMI Registry** is also indicated.

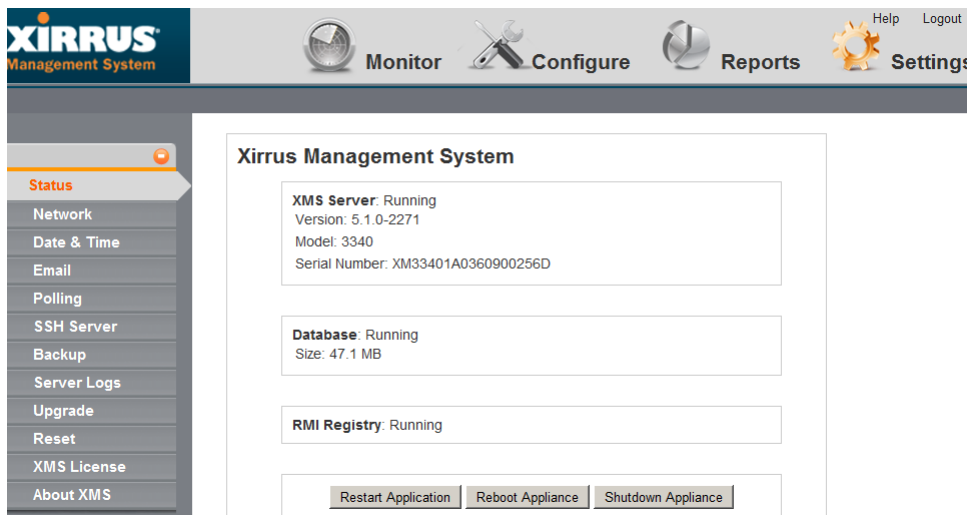


Figure 323. The Status Page

- **Restart Application**

If XMS is not running properly, you may click the **Restart Application** button on the lower left to restart the XMS server software. If the server is currently running, an orderly shutdown will be performed first.

- **Reboot Appliance**

The **Reboot Appliance** button will reboot the Management Appliance—this will shut down XMS related processes in an orderly manner before

rebooting. Rebooting and restarting will take about two minutes on a new Management Appliance. As XMS is used and the database grows, startup integrity checks will take longer. (For shutdown, see below.)

Shutting down the XMS Server

Shutting down the server incorrectly can cause problems the next time you start XMS. Use the following procedure:

1. Close all clients. You may use **Admin> Broadcast Message** in the XMS client to alert users first.
2. On the Status page, click the **Shutdown Appliance** button.
3. The Management Appliance will then gracefully shut down. A confirmation notice is displayed immediately when the shutdown process is initiated. It may take a few minutes for the Appliance to actually shut down and power itself off.

Web Client — Network Settings

Select the **Network** link on the left to display the Network Settings page. This page allows you to manage DNS settings for the server, and set the IP address and transmission parameters for the Ethernet ports.

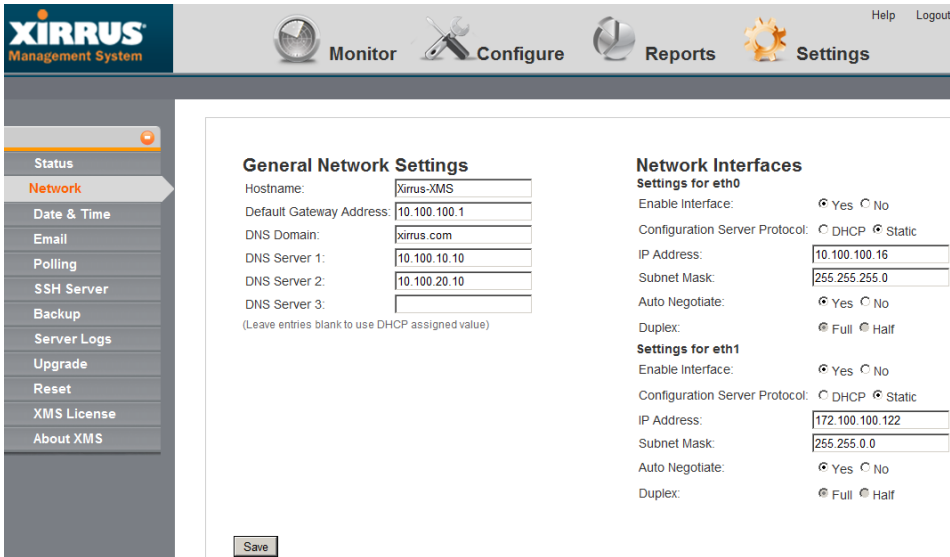


Figure 324. Changing Network Settings

***Note:** You may use one or both of the XMS Management Appliance’s Ethernet ports. If using both, then one of the ports is typically reserved for management.*

- **Network Interfaces—Settings for eth0 and eth1**

Check that **Enable Interface** is set to **Yes** for each Ethernet port that you plan to use. **Auto Negotiate** should normally be left enabled, which is the default. This will correctly set the Ethernet port’s speed and duplex mode automatically in most cases.

For recommended IP addressing, please see **“Initial Network Settings” on page 504.**

- **General Network Settings**

The **Hostname** of the Appliance is set to **xirrus-xms** by default. Note that hostnames are not case-sensitive. Xirrus Arrays send traps to the

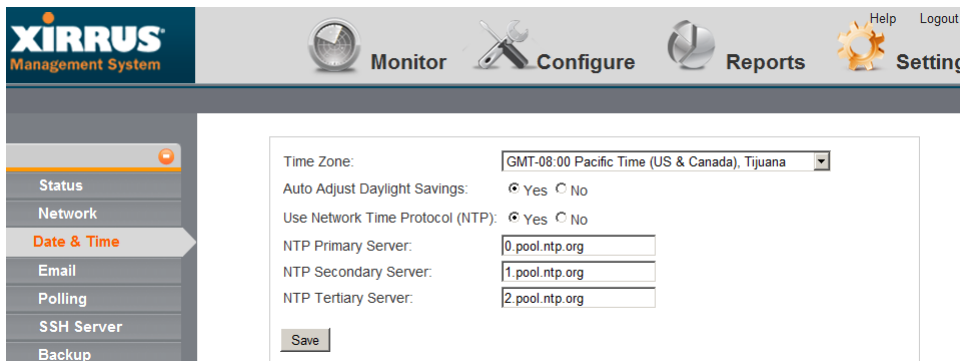
hostname **Xirrus-XMS** to announce their presence on the network and speed discovery. Thus, if you change the Appliance's DNS Hostname, you should create an alias in your network's DNS server to ensure that the Appliance is accessible using both the name **Xirrus-XMS** and your new name.

If you have clicked the **Static** radio button under **Network Interfaces - Configuration Server Protocol**, you must enter the **Default Gateway Address** for this Appliance, and enter the **DNS Domain** and **DNS Servers**.

Click the **Save** button when you have finished making your changes.

Web Client — Date and Time Settings

***NOTE:** To use SNMPv3 successfully, system time must be set using an NTP server on both the XMS server host machine and all Arrays using SNMPv3. This is because SNMPv3 requires synchronization between the XMS server and the Arrays so that the system time difference between them never exceeds more than 150 seconds. If the time difference exceeds 150 seconds, SNMPv3 suspects a security breach and removes the SNMPv3 credentials for affected Arrays from the database. This means that the Array will appear to be down and statistics will not be polled until the Array is re-discovered by scheduled discovery (unless discovery is turned off). A manual refresh of the Array should also remedy the situation. See “Scheduling Discovery” on page 74 and “Refreshing a Device” on page 88.*







XIRRUS Management System		 Monitor	 Configure	 Reports	 Settings	Help Logout
<hr/>						
Date & Time						
<div>Time Zone: GMT-08:00 Pacific Time (US & Canada), Tijuana</div> <div>Auto Adjust Daylight Savings: <input checked="" type="radio"/> Yes <input type="radio"/> No</div> <div>Use Network Time Protocol (NTP): <input checked="" type="radio"/> Yes <input type="radio"/> No</div> <div>NTP Primary Server: 0.pool.ntp.org</div> <div>NTP Secondary Server: 1.pool.ntp.org</div> <div>NTP Tertiary Server: 2.pool.ntp.org</div> <div>Save</div>						

Figure 325. Changing Date and Time Settings

Click the **Date & Time** link on the left to display the Date & Time page. This page manages your time zone and sets the time manually or sets up Network Time Protocol usage to obtain accurate time settings automatically.

- **Time Zone and Daylight Savings Time**

Select your local **Time Zone** from the pull-down list.

Enable **Auto Adjust Daylight Savings** if you want the system to adjust for daylight savings automatically, otherwise click **No**.

- **Using Network Time Protocol**

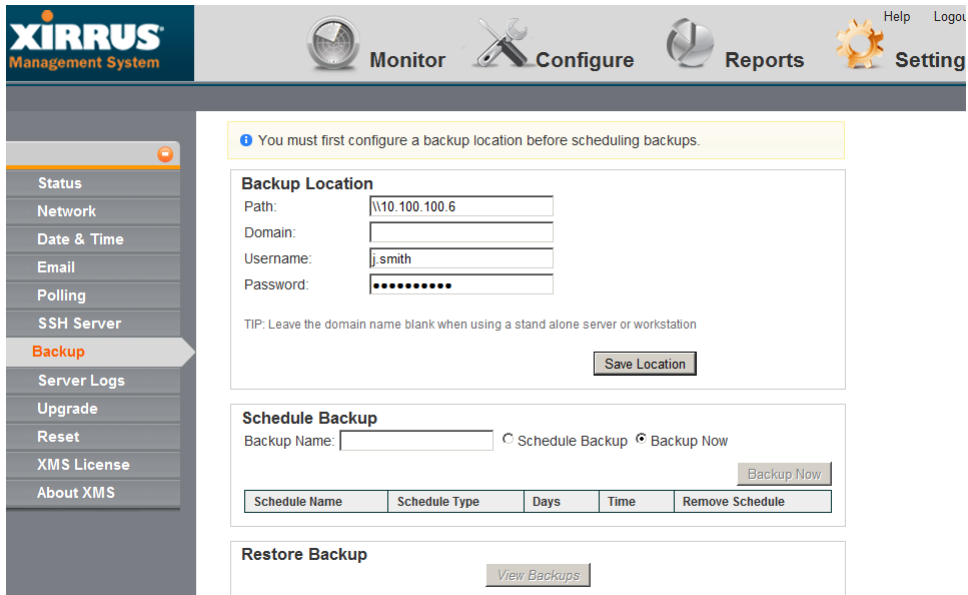
To have the time of day set automatically from an accurate time server, set **Use Network Time Protocol** to **Yes** (this is the default). You may modify the **NTP Servers** (primary, secondary, tertiary), or leave them at the default values which use NTP Pool time servers (<http://www.pool.ntp.org/>).

- **Setting time manually**

Set **Use Network Time Protocol** to **No**. Use the **Adjust Time** and **Adjust Date** fields that appear to set the correct time and date.

Click the **Save** button when you have finished making your changes.

Web Client — Database Backup Settings



Backup Location

Path:

Domain:

Username:

Password:

TIP: Leave the domain name blank when using a stand alone server or workstation

[Save Location](#)

Schedule Backup

Backup Name: ☐ Schedule Backup ☒ Backup Now

[Backup Now](#)

Schedule Name	Schedule Type	Days	Time	Remove Schedule
---------------	---------------	------	------	-----------------

Restore Backup

[View Backups](#)

Figure 326. Changing Database Backup Settings

Note: On Linux-based servers, the database and all configuration files are backed up, including any uploaded files for policies, software update, etc.

Select the **Backup** link on the left to display the Backup Location and Schedule page. This page specifies where backup files are kept and when they are to be performed. It also displays existing backups and allows you to restore from a backup file.

- **Backup Location**

Before you can use any other features on this page, you *must* specify the location for backup files.

Specify the **Path** for the folder where files are to be stored. The path may use the Windows Uniform Naming Convention (UNC) format (\\ComputerName\ SharedFolder\ Resource) or the Server Message Block Protocol (SMB) format (smb:// URL).

You may enter a **Domain** name if necessary. If the backup location is on a standalone server, you should normally leave the domain field blank.

Enter a **Username** and **Password** that will give you write privileges for that folder. While the username and password are optional, we highly recommend that the backup file server be configured to require password protection.

Click **Save Location** when done. XMS will verify that it is able to access the location and will inform you of its success or failure.

Once you have successfully specified the Backup Location, you may proceed to use the other features of the Backup page. If you have not set the Backup Location, other operations on this page may fail.

● Schedule Backup

***Note:** The command buttons in the Schedule Backups section (**Schedule Backup**, **Backup Now**, **View Backups**) are disabled until you specify a **Backup Location**.*

Enter a **Backup Name** for this entry. (**Figure 327**) If you select **Backup Now**, a backup will be performed immediately, and the backup file will be listed in the Restore Backup section below.

Schedule Backup

Backup Name:
☒ Schedule Backup
☐ Backup Now

Schedule Type:
☐ Daily
☒ Weekly
☐ Monthly

Days of Week:
☒ Sunday
☐ Monday
☐ Tuesday
☐ Wednesday
☐ Thursday
☐ Friday
☐ Saturday

Time of Day (24 hh:mm): :

Schedule Name	Schedule Type	Days	Time	Remove Schedule
monthly backup	Monthly	14	14:00	<input type="button" value="Remove"/>
schedule a back up	Daily		11:00	<input type="button" value="Remove"/>
weekly backup	Weekly	Sun, Mon, Tue, Wed, Thu, Fri, Sat	12:00	<input type="button" value="Remove"/>

Figure 327. Scheduling Backups

To create a schedule for performing backups automatically, select the **Schedule Backup** radio button after entering a **Backup Name**. Fields will be displayed to allow you to specify a schedule. (Figure 327) Select the **Schedule Type: Daily, Weekly, or Monthly**.

Depending on the selected Schedule Type, different fields will be displayed. For a monthly backup, specify the day of the month (only one day may be selected, but you can always specify more schedule entries for additional monthly backup days). For a weekly backup, check all of the days of the week on which the backup is to be performed (one or more days are allowed). For all three Schedule Types, enter the **Time of Day** for the backup. Then click the **Schedule Backup** button underneath. Your new schedule entry will be listed, showing its name and scheduled days and time. For example, Figure 327 shows an entry named Sundays which will be performed every Sunday at 2:00 AM.

To remove a schedule entry, click its **Remove Schedule** button.

- **Restore Backup**

Click the **View Backups** button to display a list of all the backup files found in the specified **Backup Location**. Each backup is identified by its **Backup Name** and **Date/Time**. (Figure 328) The most recent backup is listed first.

Restore Backup		
Backup Date/Time	Backup Name	Restore Backup
Dec 16, 2009 10:15 AM	new	<input type="button" value="Restore"/>
Dec 16, 2009 10:00 AM	sched-BU	<input type="button" value="Restore"/>
Dec 15, 2009 5:28 PM	12345	<input type="button" value="Restore"/>
Dec 14, 2009 5:55 PM	rretetet	<input type="button" value="Restore"/>
Dec 14, 2009 5:48 PM	rretetet	<input type="button" value="Restore"/>
Nov 16, 2009 5:36 PM	123456	<input type="button" value="Restore"/>

Figure 328. Restoring Backups

If you wish to restore your XMS database from a previously saved version, click the **Restore Backup** button to the right of the desired backup. You will be asked to verify that you wish to proceed.

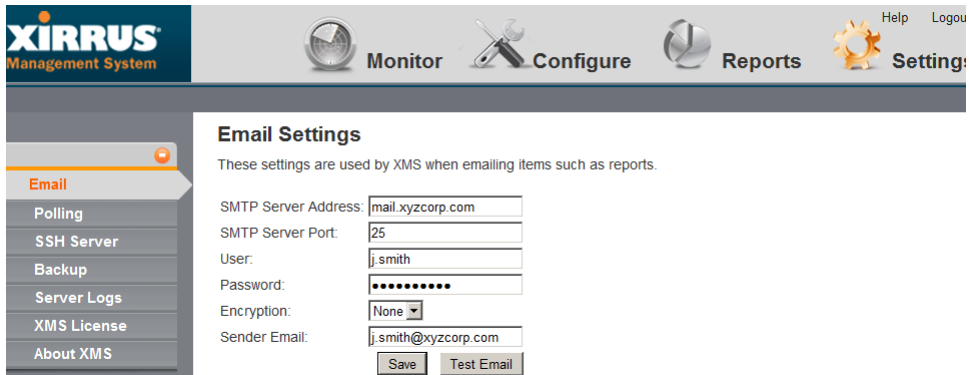
We recommend that you first notify all users that a restore will start shortly. See “**Broadcast Message**” on [page 500](#). The restore operation can impact system performance and should be scheduled for off-peak hours. After the restore operation is complete, you **must** take these actions:

- Close all XMS client applications.
- Reboot the XMS Appliance.

***Note:** To delete backups on both Linux and Windows servers, perform the deletions directly from the file system. They are found in the **Backup Location** that you specified.*

Web Client—Email Settings

Some features, such as [Viewing a Report](#), allow you to email information from XMS to yourself or others. When XMS needs to send email, it uses an SMTP server to do so. Before XMS can send any emails, you must specify which server to use and provide authentication information.



The screenshot shows the XIRRUS Management System web interface. At the top, there is a navigation bar with icons for Monitor, Configure, Reports, and Settings, along with links for Help and Logout. On the left, a sidebar menu lists various system functions: Email (highlighted), Polling, SSH Server, Backup, Server Logs, XMS License, and About XMS. The main content area is titled "Email Settings" and includes a descriptive sentence: "These settings are used by XMS when emailing items such as reports." Below this, there are input fields for SMTP Server Address (mail.xyzcorp.com), SMTP Server Port (25), User (j.smith), Password (masked with dots), Encryption (set to None), and Sender Email (j.smith@xyzcorp.com). At the bottom of the form are two buttons: "Save" and "Test Email".

Figure 329. Changing the Email Server

To specify the SMTP server for XMS to use, click **Settings** at the top of the page and then use the **Email** link on the left. ([Figure 329](#))

Enter your **SMTP Server Address** and **SMTP Server Port**. Specify the **User** and **Password** that XMS must use to access the server. Select an **Encryption** type.

When XMS sends an email, it will identify it as being sent from the email address that you specify in the **Sender Email** field. You may click the **Test Email** button to verify that you have specified the SMTP server correctly. Enter your email address in the dialog box that appears to check that XMS is able to use SMTP to successfully send an email.

Click **Save** when done.

Web Client — Polling Settings

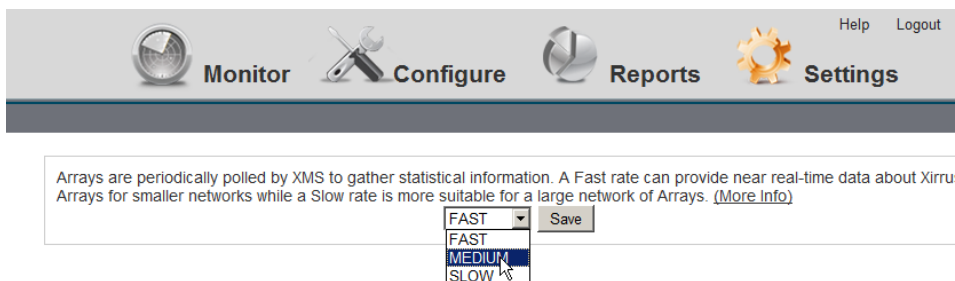


Figure 330. Changing Polling Rate

Click the **Polling** link on the left to display the Polling page. This page changes the rate at which various types of network information are updated. Note that for Windows-based XMS servers, you may change polling frequency using XSMT as described in “[Changing Polling Frequency](#)” on page 537.

XMS offers a rich set of statistics in its **Dashboard**, **Reports**, and other windows. These statistics are obtained by polling the managed Arrays using SNMP. The default polling rate is **FAST**, providing near real-time data. If you have a large number of Arrays under management, we recommend that you decrease the polling speed to enhance XMS performance. Select **FAST**, **MEDIUM**, or **SLOW** from the drop-down list and click the **Save** button.

The following table summarizes the polling intervals used for the three polling rates.

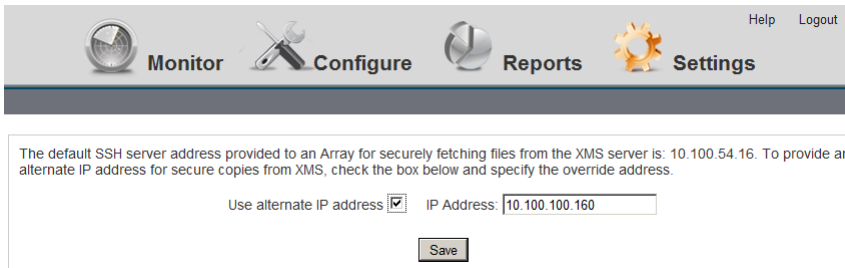
Item	Polling Interval FAST	Polling Interval MEDIUM	Polling Interval SLOW
Array Up/Down Status	1 minute	5 minutes	5 minutes
Statistics	40 seconds	80 seconds	120 seconds
Station Counts	40 seconds	80 seconds	120 seconds
Rogues	150 seconds	300 seconds	450 seconds

The following table summarizes the recommended polling intervals for various network sizes.

Polling Rate	Number of Arrays
Fast	up to 100
Medium	up to 250
Slow	over 250

After you change the polling rate, each Array will be reconfigured for the new polling interval. Depending on the number of Arrays under management, it might take some time to process the change on all Arrays (up to 10 seconds per Array). You may continue to use XMS while this change is proceeding.

Web Client — Changing the SSH Server Address



The screenshot shows the XIRRUS Web Client interface. At the top, there is a navigation bar with icons and labels for Monitor, Configure, Reports, and Settings. The Settings tab is selected. Below the navigation bar, there is a text box explaining the default SSH server address and the option to use an alternate IP address. The 'Use alternate IP address' checkbox is checked, and the 'IP Address' field contains the value '10.100.100.160'. A 'Save' button is located at the bottom of the form.

Figure 331. Changing the SSH Server

Some policies, such as **Software Update** and **Web Page Redirect (WPR)**, require Arrays to download files. When XMS instructs an Array to fetch a file from the server, the Array opens an SSH session with the XMS server to perform a secure transfer of the file. By default, XMS instructs the Array to connect to the XMS server's IP address. In some situations you may need to specify a different externally accessible IP address, for example if NAT is in use on the XMS server's network.

To change the IP address that Arrays will be instructed to use for an SSH connection, use the **SSH Server** link on the left. Note that the current SSH server

address is displayed. (Figure 331) Click the **Use alternate IP address** checkbox and enter the desired **IP Address**. Click **Save** when done.

Note that Arrays will use Port 22 for SSH to the XMS server.

Web Client — Viewing Server Log Files

		Export
Log File	Log Size	
alert_audit.txt	46 KB	
ConfChange_log	8 KB	
ConfChange_log.old	8 KB	
ConfChangeErr_log	0 KB	
ConfChangeErr_log.old	0 KB	
mserr.txt	4 KB	
msout.txt	6 KB	
mysql_repair_result.txt	16 KB	
nmserr.txt	168 KB	
nmsout.txt	267 KB	
nmsout.txt.1	1024 KB	
stderr.txt	215 KB	
stdout.txt	104 KB	
transactionLogs.txt	649 KB	
updateManagerlog.txt	0 KB	
updateManagerlog1.txt	0 KB	

Figure 332. Viewing Log Files

Use the **Server Logs** link at the left to display the Logs page. This page displays a link for each of the working log (message) files generated by the XMS server while it is running. Click a link to view the contents of that file. (Figure 333) These files journal the operation of the XMS server software, rather than reporting on the operation of the Wi-Fi network.

Log files are intended for use by Xirrus Customer Support personnel. In certain situations, Support personnel may ask you to send them some of these files. Use the **Export** button to save log files to your file system. If you click this button on the Logs page (the page showing the list of log files), then XMS creates a zip file containing all of the logs. If you click **Export** on a page for a particular log file, then XMS creates a .csv file for that log. In either case, a dialog allows you to open or save the file and browse to the desired location for saving the export file. If you choose to open a .csv file rather than saving it and you have Excel installed on your workstation, an Excel window opens and displays the log file contents.

```
----- Logging started -----
Messages on *****Tuesday, December 22, 2009*****
-----General Information-----
Product = Management System webclient.performance.reports.period=Period
Service Pack Version =AdventNet_Web_NMS-4.7-SP.X X X-XXX
Feature Pack Name = Syslog_Monitoring
Feature Pack Version = AdventNet_Web_NMS-4.5-Syslog-FP-2.0
os name=Windows XP
os version=5.1
os architecture=x86
java version=1.6.0_01
java vendor=Sun Microsystems Inc.
java specification=Java Platform API Specification
java specification version=1.6
java vm name=Java HotSpot(TM) Client VM
java vm information =mixed mode
java compiler=null
*****

(TID=75 LVL=INFO) Starting WorkflowProcess
(TID=75 LVL=INFO) Workflow process configured: 5 thread(s), purge enabled, purge interval 120 min
com.xirrus.xms.server.event.ServerTopicPublisherFactory
```

Figure 333. Viewing a Selected Log File

If a listed log files grows too large, it is closed and renamed and a new file is started. The following example illustrates this on a Linux-based Management Appliance. As shown in **Figure 334**, there are four **xirrusout.txt** files.

- **xirrusout.txt** contains the most recent entries.
- **xirrusout.txt.1**—the first time that xirrusout.txt grows too large, it is closed and renamed to xirrusout.txt.1. A new xirrusout.txt is created to capture ongoing new entries.
- **xirrusout.txt.2**—the second time that xirrusout.txt grows too large, it is closed and renamed to xirrusout.txt.2. Thus xirrusout.txt.1 contains the oldest entries, and xirrusout.txt.2 has the next oldest entries, etc. The number of log files is limited to 10 or 20 instances, depending on the log file type.

xirrusout.txt	818 KB
xirrusout.txt.1	1025 KB
xirrusout.txt.2	1024 KB
xirrusout.txt.3	1024 KB

Figure 334. Multiple Log Files

Web Client—Managing the XMS Server License



This section describes the license to use the XMS server. If you are looking for information regarding using XMS to manage Array licenses, please see “Managing Array Licenses” on page 189.

For full operation, the XMS server must have a license installed. Until the license is installed, the server will operate in a default mode that allows it to manage only one Array. Thus, without an appropriate license, **Discovery** will stop at one Array and will not allow more Arrays to be added. If you do not have a valid license, you will be notified each time you start an XMS client.



Valid XMS licenses are typically for a particular number of Arrays. When XMS has discovered the maximum permitted number of Arrays, no additional Arrays will be discovered.

Use the following steps to enter your license.

1. Click the **Settings** button, then click **XMS License** on the left. The XMS License Info page appears.

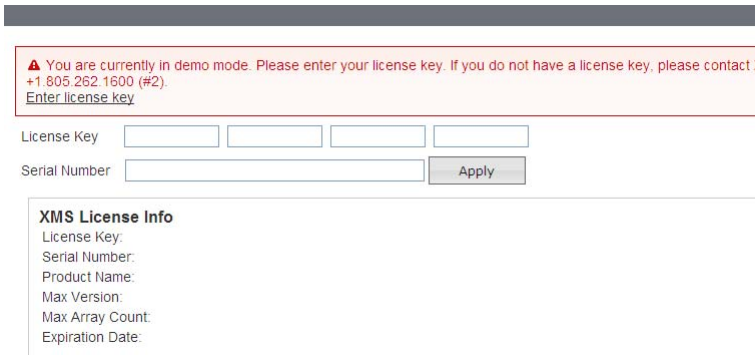


Figure 335. XMS Server License

2. Xirrus will supply you with a **License Key** and **Serial Number** for your server. Enter **both** of these fields exactly as they were provided to you (the fields are not case-sensitive), and click **Apply**.

3. After processing the license information, the following additional fields will be shown:
 - Product Name—XMS server's product name.
 - Max Version—the highest release number supported by this license. All incremental upgrades to the release shown are also supported. For example, if Max Version is 5.0, then this license will run Release 5.0.999, but Release 5.1 will require an updated license.
 - Max Array Count—the server is licensed to manage a specific maximum number of Arrays. To manage additional Arrays, please contact Xirrus to upgrade your license.
 - Expiration Date—the date that this license expires.

Web Client — Performing Upgrades



Figure 336. Upgrading XMS Software

Select the **Upgrade** link on the left to display the Upgrade page. This page allows you to update the XMS server software.

When you receive updated software from Xirrus, it comes in the form of a .tar file. For example:

```
xms-5.0.0-1951.tar
```

An upgrade file for a Linux-based server contains an entire software upgrade, rather than having an incremental patch that depends on previous patches being installed. Please follow the instructions furnished with the release carefully. The XMS server must be stopped before you can perform an upgrade.

When you receive a new release file from Xirrus, place it where you will be able to browse to it from the web browser where you are running the web client. Warn all XMS clients (see **“Broadcast Message” on page 500**) that the XMS server will be going down (but do not stop the XMS server, or you will lose your access to the web client!). Next, click the **Browse** button to browse to the .tar file. Click **Upgrade** to install the new software.

When the process is complete, a pop-up message will be displayed. It will inform you that you must reboot the Appliance. Click the **OK** button to close it. The new release becomes the current version of the XMS server.

Web Client — Resetting the XMS Server

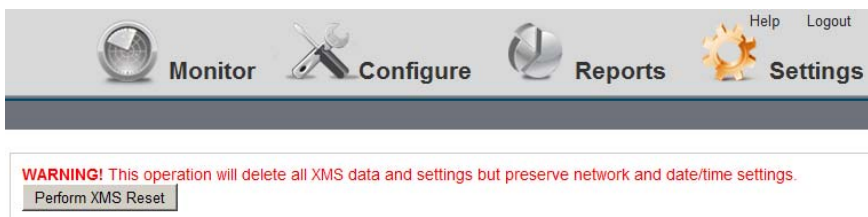


Figure 337. Resetting XMS

Use the **Reset** link at the left to display the Reset page. This page allows you to perform a reset on the server. This deletes all data in the XMS database (but it does not delete backup files). It also returns the XMS server back to all of its factory default settings, except that **Web Client — Network Settings** and **Web Client — Date and Time Settings** are retained.

Click the **Perform XMS Reset** button to perform the reset. You will be asked to verify that you wish to proceed.

When the reset is complete, your first action should be to specify **Web Client — Database Backup Settings**.

Managing XMS on Windows-based Systems

On the XM-3300 and XA-3300-CC, the Xirrus Server Management Tool (XSMT) is used to start, stop, or view the status of the server, install patches, and for advanced settings and database management. The web client may also be used for managing some settings. XMS server management is discussed in the following sections.

- “Starting the XMS Server on Windows-based Systems” on page 524
- “Xirrus Server Management Tool (for Windows-based Servers)” on page 526
- “Managing XMS Server Settings via the Web Client” on page 540

Figure 338 shows XSMT’s XMS Server Manager window when the server is up.

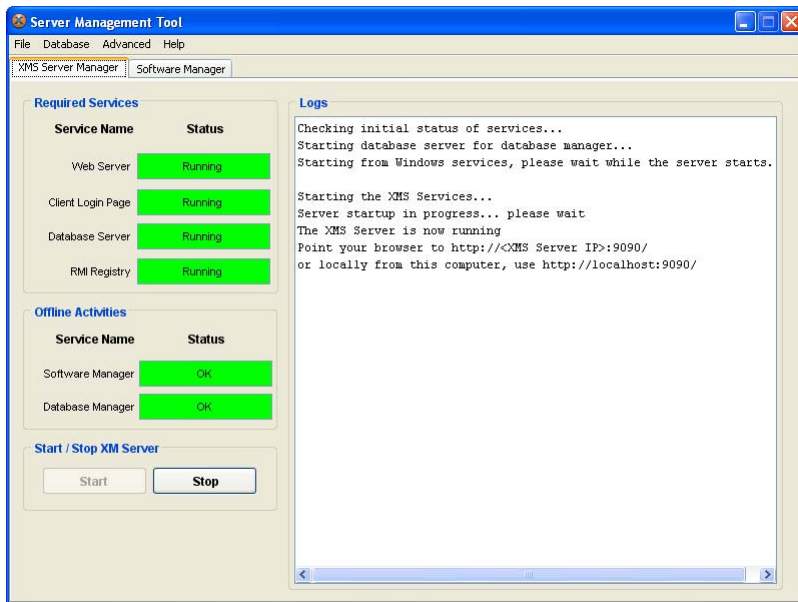


Figure 338. Xirrus Server Management Tool - XMS Server Manager

The XMS server typically runs as a Windows service, and is listed along with other Windows services accessible from Windows Administrative Tools. You may view the status of the XMS server in this way, but we recommend that you start or

stop the server using XSMT rather than as a Windows Service, so that you can monitor status.

Starting the XMS Server on Windows-based Systems

In the installation process, there are options to have the XMS server start automatically, or to wait for the administrator to explicitly start it. To see whether the XMS server is running correctly, use XSMT.

If XSMT is not running, start it using the Windows **Start** button > **All Programs** > **Xirrus** > **Xirrus Management System** > **XA-3300-CC**. The XSMT window is displayed. (Figure 338)

- **Starting XSMT on the XM-3300-CC**

When you log in to the XM-3300 (the default login is **Administrator/Xirrus!23**), the Xirrus Server Management Tool is automatically started and the XSMT window is displayed.



At other times, if XSMT is not running, you may start it by clicking the XSMT shortcut icon on the Windows desktop.

- **Starting XSMT on your server with XA-3300-CC installed**

From the Windows Start menu, select **All Programs** > **Xirrus** > **Xirrus Management System** > **XA-3300-CC**.

The first time that you start XSMT, a message will appear asking whether you wish to configure XMS to run as a Windows Service. Click **Yes**.

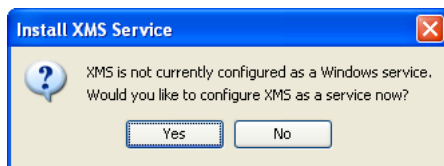


Figure 339. Start XMS as a Windows Service

Wait for the **Start** button on the lower left to be enabled, then click it to start the XMS server.

During server initialization, the XSMT Logs panel displays high-level progress messages.

When XMS server startup is finished, the XMS Server Manager tab of XSMT will indicate that the server is up and running. **Figure 338 on page 523** shows an example of a successful server initialization process. The state of all servers is **Running** and they are shown in green.

When the XMS server is ready for clients to be started, the Logs section on the right of the window will display:

```
*** The XMS Server is now running
Point your browser to http://<XMS Server IP>:9090/
or locally from this computer, use http://localhost:9090/
```

When the server starts for the first time, it will initialize the database. Discovery is not started automatically—you should start the discovery process to add Xirrus Arrays and PoGE injectors to the XMS database (see **“Discovering the Network” on page 67**).

The first time that XMS starts, you should use the Backup Manager to establish a backup schedule for the database. See **“Backup Manager” on page 499**. For more information on using XSMT, see **“Xirrus Server Management Tool (for Windows-based Servers)” on page 526**.

Xirrus Server Management Tool (for Windows-based Servers)

This tool is provided to manage the XMS server and to perform certain advanced operations.

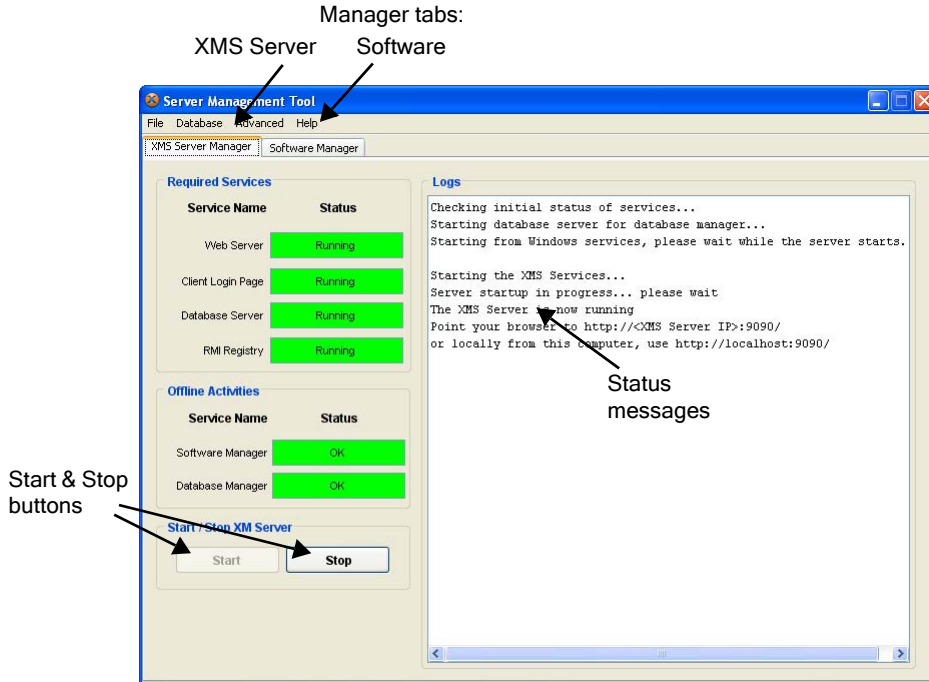


Figure 340. Xirrus Server Management Tool - XMS Server Manager

XSMT has two major functions, each one with its own tab, plus advanced menu options:

- **XSMT - XMS Server Manager Tool**—displays server status and starts and stops the server.
- **XSMT - Software Manager**—updates XMS server software with new releases.
- **XSMT - Database Tools**—these menu options initialize or repair the database.

- **XSMT - Advanced Settings**—these menu options change polling intervals and the SSH server address.

Note: XMS has a browser-based interface which may be used to manage some server settings. See “Managing XMS Server Settings via the Web Client” on page 540.

XSMT - XMS Server Manager Tool

The XMS Server Manager window is divided into two distinct areas:

- **Status**—The **Required Services** and **Offline Activities** sections show the status of the various services that are part of or associated with the XMS server. The Start / Stop XMS Server section at the bottom starts or stops the server.
- **Logs**—shows the actions taken such as starting and stopping services, and when the action is complete.

Required Services

This section shows the running status of the major XMS services.

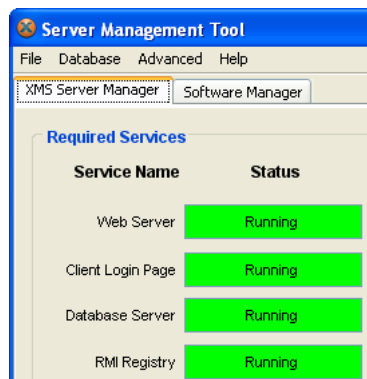


Figure 341. Status of Services, Showing Normal Status

Required services include:

- **Web Server**—the main server used by XMS clients.
- **Client Login Page**—authenticates XMS client login requests. If this service is down, clients will be unable to log in even if the rest of the XMS server is running.

- **Database Server**—all XMS data is handled by this server. You may manage it from the client or the server. See **“Backup Manager” on page 499** and **“XSMT - Database Tools” on page 532**.
- **RMI Registry**—used internally for communication between XMS subsystems.

The possible status values for these services may be:

- **Running** (Green)—the service is running properly.
- **Not Running** (Yellow)—the service has been stopped, either by administrator request or by error. Yellow is also used during the start-up and shut-down transition states. Check the **Logs** portion of the window for more information.
- **Checking...**(Gray)—shown during startup as XSMT is checking the state of the service and starting it if necessary.

Offline Activities

This section shows the running status of XMS managers. Activity on a manager may be started by an XMS administrator.

Offline Activities	
Service Name	Status
Software Manager	OK
Database Manager	OK

Figure 342. Status of Offline Activities

Offline activities include:

- **Software Manager**—used to install XMS software updates. See **“XSMT - Software Manager” on page 534**.
- **Database Manager**—this is used to manage backups. See **“Backup Manager” on page 499**.

The possible status values for these services may be:

- **Checking...**(Gray)—shown during startup as XSMT is checking the state of the manager and starting it if necessary.

- **OK** (Green)—there is currently no action in progress (idle but ready).
- **Not Running** (Yellow)—the service has been stopped, either by administrator request or by error. Yellow is also used during the start-up and shut-down transition states. Check the **Logs** portion of the window for more information.
- **Restore In Progress** (Database Manager, Yellow)—a database restore is running. It must complete before the XMS server can be started.
- **Patch In Progress** (Software Manager, Yellow)—a software update is in progress. It must complete before the XMS server can be started.

XSMT - Starting the XMS Server

The XMS server must be running if you want to serve XMS clients, but remember that the server must be stopped if you want to perform advanced database operations ([Re-initialize](#) and [Repair](#)).

To start the server from the Xirrus Server Management Tool any time the server is down, select the XMS Server Manager tab and click the **Start** button on the lower left. When the server begins its startup process, the Logs section on the right of the window displays the progress of the system operations that are completed. XSMT also opens a system console window in which you can watch progress in more detail ([Figure 343](#)). To review the full content of the console window, use the scroll bar.

Note that the **Start** button will be disabled if the server is running or if the current status of the server is not properly shut down. To stop the server, see [“XSMT - Shutting Down the XMS Server” on page 531](#).

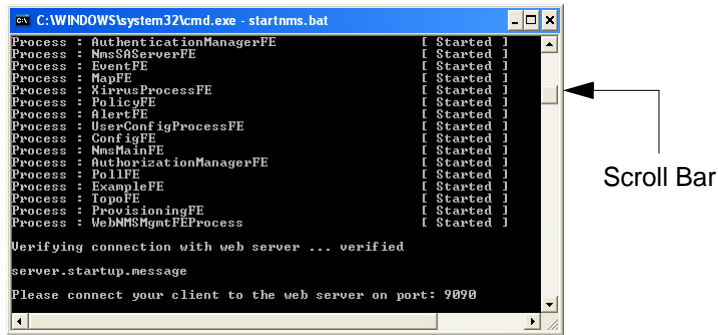


Figure 343. Server Startup Progress

When the server has been started successfully, the status of all the **Required Services** will be **Running** (green) as shown in **Figure 344**.

When the XMS server is up, the Logs portion of the window will show the following messages:

```
*** The XMS Server is now running
Point your browser to http://<XMS Server IP>:9090/
or locally from this computer, use http://localhost:9090/
```

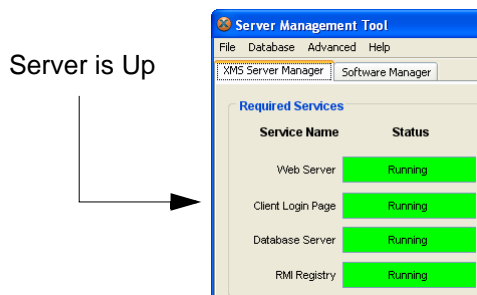


Figure 344. Server is Up (XSMT)

XSMT - Shutting Down the XMS Server

You can shut down the server at any time using the Xirrus Server Management Tool, or the server can shut down automatically if it detects a problem. The server must be shut down before you can initiate the following advanced database operations: [Re-initialize](#) and [Repair](#).

To shut down the server, select the XMS Server Manager tab in the XSMT window and click the **Stop** button on the lower left. The Shutdown Server window is displayed, which requires you to enter a user name and password—the default for both is **admin**. Click on the **Submit** button to initiate the server shutdown process. Note that the **Stop** button will be disabled if the server is not running or if the current status of the server will not permit shut down.

***Note:** In rare instances, the XMS server may be unable to start, and the **Stop** button will be disabled. In this case, you may use the **File > Kill server** menu option to kill all server processes. This should be used **only** as a last resort! The **Stop** button does an orderly shutdown—if it is enabled, it should **always** be used instead of the **Kill** option.*

When the server begins its shutdown process, the Logs section on the right of the XSMT window displays the progress of the system operations that are completed. (**Figure 345**) XSMT displays the system console window, in which you can watch progress in more detail. To review the full content of the console window, use the scroll bar.

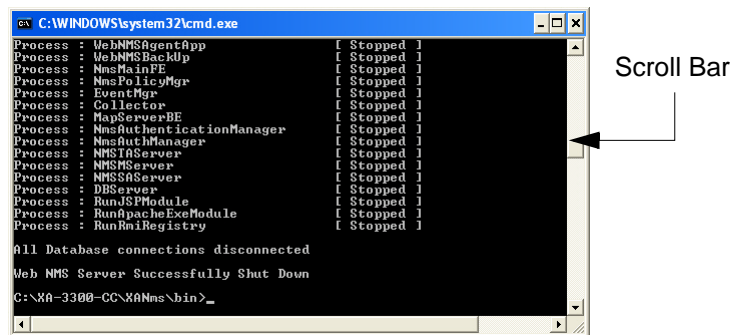


Figure 345. Server Shutdown Progress

When the server has shut down successfully, the Start button in XSMT will be enabled, and the system console window will say:

```
WebNMS Server Successfully Shut Down
```

The database server will still be running after the XMS server is shutdown.

Required Services	
Service Name	Status
Web Server	Not Running
Client Login Page	Not Running
Database Server	Running
RMI Registry	Not Running

Figure 346. Status for Stopped XMS Server

XSMT - Database Tools

Although you can view, schedule, or restore database backups from any client using the **Backup Manager**, you can only **Re-initialize** or **Repair** the XMS database using XSMT. These management tasks are available on the **Database** menu in XSMT. For an overview of other database features, please see **“About the XMS Database” on page 501**.

When the XMS server is up and running (i.e., the Web Server, Client Login Page, and RMI Registry are running), the initialize and repair options are disabled. You will receive an informational message if you try to use them, notifying you that you must stop the server first.

- **Re-initialize Database**

Choose this option if you want to re-initialize the current database, which means clearing the database. See **“Re-initialize Database” on page 532**.

- **Repair Database**

Choose this option to attempt to repair the current database. See **“Repair Database” on page 533**.

Re-initialize Database

This operation clears the database. All of your configuration, discovery, statistics, and other data will be lost. When you select this operation, XMS starts the

database server if it's not already running, and deletes all XMS tables. When the XMS server restarts, it finds that the database is empty and initializes the database for its use.

Although this tool is available in XSMT, re-initializing a database should only be performed in these situations:

- When the Release Notes for a new version of XMS explicitly instruct you to re-initialize the database when upgrading from your currently running release.
- As a last resort, it can be used to recover from catastrophic database corruption. Please call Xirrus Customer Support before re-initializing.

To re-initialize the database, first **shut down** the XMS server and then select **Re-initialize** from the XSMT **Database** menu. You are presented with a message warning you that all data and configuration information stored in the database will be deleted before it can be re-initialized. Click on the **Yes** button to proceed with the re-initialization process, or click on the **No** button to abort the process.

If you clicked on the **Yes** button and started the re-initialization process, the server console window displays the progress of the system operations that are completed. You can review the full content of the console window by using the scroll bar. When the database initialization process is completed, a confirmation window is displayed. Click on the **OK** button to close the window.

Repair Database

This operation checks the internal indexing in the database and attempts to repair any problems.

Although this tool is available in XSMT, you should only repair the database if it has been corrupted. If the database is damaged, it may not allow you to restore from a backup. So if there is actual table corruption, it needs to be repaired prior to restoring any backup. Please contact Xirrus Customer Support before repairing the database.

To repair the database, first **shut down** the server and then select **Repair database** from the **Database** menu. You are presented with a message verifying that you wish to proceed. Click **Yes** to proceed, or click **No** to abort the process.

When the database repair process is completed, a confirmation window is displayed. Click on the **OK** button to close the window. You may then restart XMS (see “**XSMT - Starting the XMS Server**” on page 529).

***Note:** There is an optional external script available for performing repair operations. The advantage of using the script is that it creates a log file that can be reviewed to determine if any problems remain, and which problems were actually repaired. Contact Xirrus customer support for more information. See “**Contact Information**” on page 544.*

XSMT - Software Manager

The Software Manager tab of XSMT allows you to install new release versions (called patches) of the XMS server, or revert to a previously installed release.

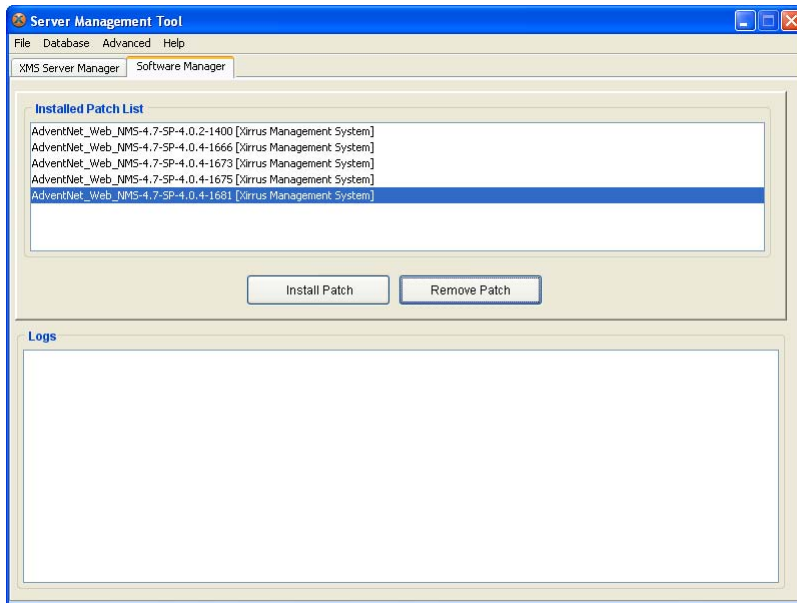


Figure 347. XSMT Software Manager

When you receive updated software from Xirrus, it comes in the form of a “patch” file with a .ppm file extension. For example:

```
xms-XA-patch-5.0.0-1953.ppm
```

Patches may be dependent on each other - i.e., one release may depend on other files being installed first, and the order in which they are installed may be important. Please follow the instructions furnished with the release carefully. The XMS server must be stopped before you can perform any Software Manager operations.

About the Installed Patch List

When a new release is installed, it is added to the bottom of the Installed Patch List and becomes the running version of the XMS server. The last (bottom) release in this list is always the running version.

If you select a release in the list and click the **Remove Patch** button, that release **and all later releases** (all the entries below it) are removed. When you start the XMS server again, it will run the release version that is currently at the bottom of the Installed Patch List.

To Install a New Version of the XMS Server

When you receive a new release file from Xirrus, place it where you will be able to browse to it from the XMS server computer. Warn all XMS clients (see **“Broadcast Message” on page 500**), then **shut down** the XMS server and go to the Software Manager tab in XSMT. Then click the **Install Patch** button. The Select Patch File dialog box appears.

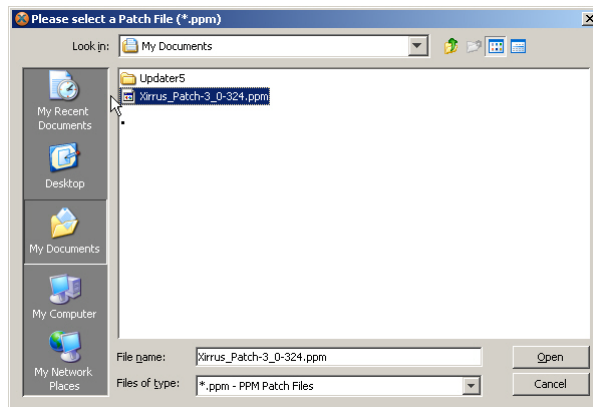


Figure 348. Select a Patch File

Browse to the new **.ppm** file and click **Open**. The new release will be installed. The Logs section of the Software Manager window shows output from the installation process. When the process is complete, a pop-up message will be displayed. Click the **OK** button to close it. The new release becomes the current version of the XMS server. The file appears at the bottom of the Installed Patch List.

Close XSMT if it doesn't close automatically after installing a patch, and relaunch it (since the patch may have affected XSMT). You may then start the XMS server (see [“XSMT - Starting the XMS Server” on page 529](#)).

To Remove a Patch

The **Remove Patch** button may be used to remove the most recently installed release, or the last few releases installed. The release remaining at the bottom of the Installed Patch List will be used as the running version when the XMS server is restarted. See [“About the Installed Patch List” on page 535](#). You cannot remove the first (top) entry in the list.

To remove one or more releases, **shut down** the XMS server and go to the Software Manager tab in XSMT. Decide which of the installed releases you would like to have as the running version, and click the entry beneath that in the Installed Patch List. Then click the **Remove Patch** button. You will be asked to verify the removal. The selected file and all of the files underneath it will be removed from the Installed Patch List. A pop-up message will inform you when the removal is complete. Click **OK** to close it.

When the removal is complete, XSMT shuts down. (If it does not close automatically, you should shut it down manually.) Relaunch XSMT before proceeding to do anything else with XMS. You may then start the XMS server (see [“XSMT - Starting the XMS Server” on page 529](#)). The version at the bottom of the Installed Patch list will be used.

XSMT - Advanced Settings

The **Advanced** menu in XSMT allows you to change settings in the XMS server, in order to modify the polling interval for Arrays and to change how the server communicates with Arrays via SSH.

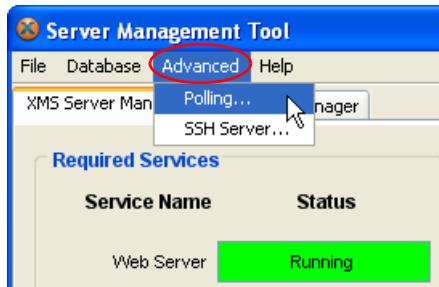


Figure 349. XSMT Advanced Menu Options

The Advanced menu provides two functions:

- **Changing Polling Frequency**
- **Changing the SSH Server Address**

There is also a browser-based interface that allows you to change XMS server settings:

- **Managing XMS Server Settings via the Web Client**

Changing Polling Frequency

XMS offers a rich set of statistics in its **Dashboard**, **Reports**, and other windows. These statistics are obtained by polling the managed Arrays using SNMP. The default polling rate is **Fast**, providing near real-time data. The **Advanced > Polling** menu option allows you to change the polling interval that the XMS server uses. Note that you may also change polling frequency using the web client, as described in **“Web Client — Polling Settings” on page 516**.

If you have a large number of Arrays under management, we recommend that you increase the polling interval to enhance XMS performance. The following table summarizes the recommended polling intervals for various network sizes.

Polling Rate	Number of Arrays	Base interval multiplied by
Fast	0 to 100	1
Medium	100 to 250	2
Slow	Over 250	3

To change the polling interval at any time when the XMS Server is running, select **Polling** from the **Advanced** menu. Drag the slider (**Figure 350**) to the preferred polling speed, as suggested in the table above. Click **Save** when done. The polling rate may only be changed when the XMS server is running.

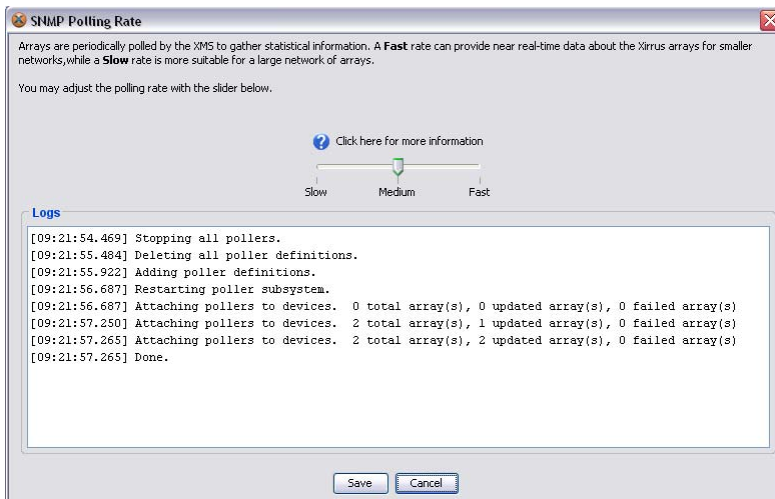


Figure 350. Changing Polling Frequency

After you change the polling rate, each Array will be reconfigured for the new polling interval. The Polling Rate window will display the progress of this process. Depending on the number of Arrays under management, it might take some time to process the change on all Arrays (up to 10 seconds per Array). You may continue to use XMS while this change is proceeding.

If you are using the browser interface to manage polling speed, proceed as described in “**Web Client — Polling Settings**” on page 516.

Changing the SSH Server Address

The **Software Update** and **Web Page Redirect (WPR)** policies require Arrays to download files. When XMS instructs an Array to download a file from the server, the Array opens an SSH session with the XMS server to perform a secure transfer of the file. By default, XMS instructs the Array to connect to the XMS server's IP address. In some situations you may need to specify a different externally accessible IP address, for example if NAT is in use on the XMS server's network.

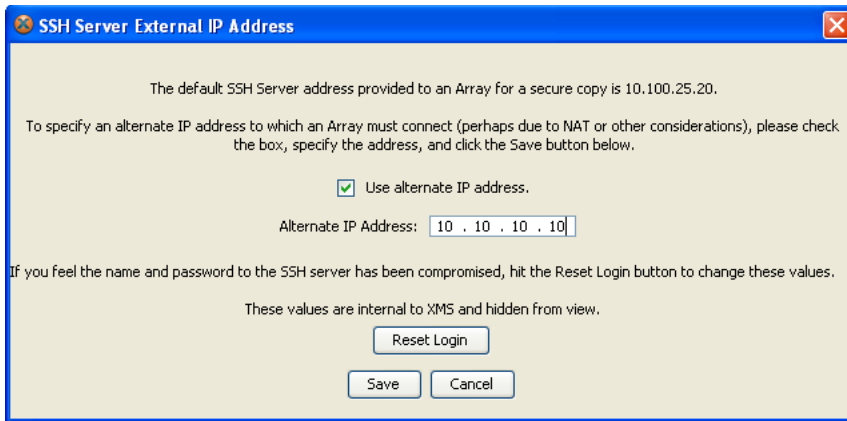


Figure 351. Changing the SSH Server

To change the IP address that Arrays will be instructed to use for an SSH connection, select **SSH Server** from the **Advanced** menu. Note that the dialog box displays the current SSH server address. (**Figure 351**) Click the **Use alternate IP address** checkbox and enter the desired **Alternate IP Address**.

If you need to reset the SSH server's login because you think the name and password may have been compromised, click the **Reset Login** button. Click **Save** when done.

Note that the Arrays always use Port 22 for SSH.

If you are using the browser interface to change the SSH server settings, proceed as described in **“Web Client — Changing the SSH Server Address” on page 517**.

Managing XMS Server Settings via the Web Client

The XMS web client also allows you to change some XMS server settings. Access it in the same way as described in [“Accessing the Web Client” on page 503](#).

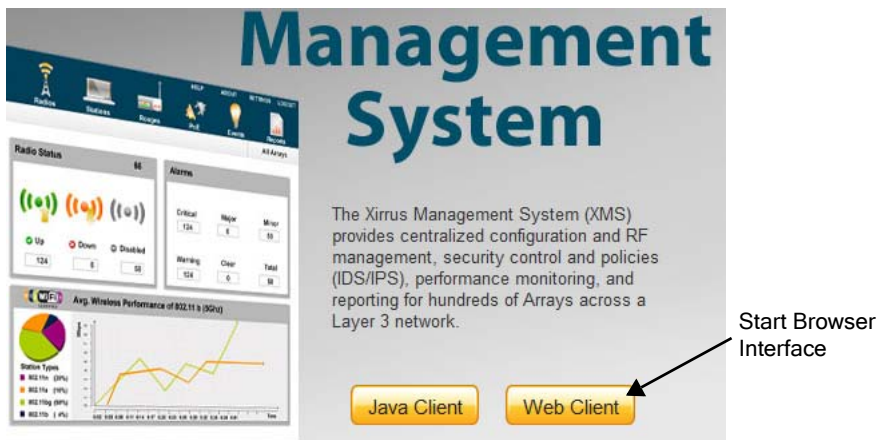


Figure 352. Changing Advanced Settings from a Browser

This interface is the same as the one used for [Managing XMS on Linux-based Management Appliances](#), except that it does not include the pages that are only used for managing Linux-based XMS servers. It has the following links, which are used exactly the same way as they are in the web client:

- **Backup**—see [“Web Client — Database Backup Settings” on page 511](#).
- **Polling**—see [“Web Client — Polling Settings” on page 516](#).
- **SSH Server**—see [“Web Client — Changing the SSH Server Address” on page 517](#).
- **Server Logs**—see [“Web Client — Viewing Server Log Files” on page 518](#).
- **XMS License**—see [“Web Client—Managing the XMS Server License” on page 520](#).

Technical Support

This chapter provides valuable support information that can help you resolve technical difficulties. Before contacting Xirrus, review all sections in this chapter and try to determine if your problem resides with XMS, the server platform, or your network infrastructure. Section headings for this chapter include:

- **“General Hints and Tips for Xirrus Management Appliances” on page 541**
- **“Frequently Asked Questions” on page 542**
- **“Contact Information” on page 544**

General Hints and Tips for Xirrus Management Appliances

This section provides some useful tips that will optimize the reliability and performance of XMS.

- You must terminate all applications before shutting down the server Appliance. This includes closing down the client interface and the server. For more information, go to **“Shutting Down the XMS Server” on page 38**.
- For best performance, the Management Appliance should be mounted in a dust-free and temperature-controlled environment.
- Ensure that the Management Appliance receives adequate ventilation at all times. The unit’s cooling fans are mounted on the rear panel. Do not obstruct the fans.
- Never use the Management Appliance chassis as a base for heavy monitors or other equipment.
- Some Appliance management operations may take a few minutes to complete. Always be patient and wait for these operations to finish before attempting another task.

Frequently Asked Questions

This section answers some of the most frequently asked questions regarding the functions and operation of XMS.

Q. Why won't my browser connect to the XMS server to start the XMS client? I can ping the server.

A. Remember to point the browser to Port 9090 on the server by appending :9090 to the server address. For example:

http://192.168.10.40:9090

Also note that if you selected a different port for accessing the XMS server during installation of the XMS server software, then you must append that port number to the URL instead of 9090.

Q. Why will XMS not discover an Array, even though the Array is connected to the network and functioning correctly?

A. SNMPv2 or v3 (Simple Network Management Protocol) must be enabled on the Array. Log in to the Array and check the SNMP settings. If the problem persists, check that the Array is on the same subnet as the XMS server.

For discovery of a device (Array or PoGE injector), the device must have SNMP enabled and its community string must match one of the strings listed in the Discovery window. See [“SNMPv2 And SNMPv3 Settings” on page 482](#). The default SNMPv2 community string in XMS matches the Array default value.

When an Array boots up, it sends an SNMP trap to the XMS server's default hostname, **xirrus-xms**. XMS can then add it to its discovered devices list. This Phone Home feature requires DNS to resolve the hostname xirrus-xms correctly. Thus, if you change the host name of the XMS server, you must configure DNS to resolve xirrus-xms to the actual name of the XMS server host.

- Q. XMS discovered my Array using SNMPv3, and the Array has connectivity and is running OK, but XMS reports that the Array is down.**
- A.** To use SNMPv3 successfully, system time must be set using an NTP server on both the XMS server host machine and on all Arrays using SNMPv3. This is because SNMPv3 requires synchronization between the XMS server and the Arrays so that the system time difference between them never exceeds more than 150 seconds. If the time difference exceeds 150 seconds, SNMPv3 suspects a security breach and removes the SNMPv3 credentials for affected Arrays from the database. This means that the Array will appear to be down and statistics will not be polled until the Array is re-discovered by scheduled discovery (unless discovery is turned off). A manual refresh of the Array will also remedy the situation. See [“Scheduling Discovery” on page 74](#) and [“Refreshing a Device” on page 88](#).
- Q. When managing large Array deployments, will the performance of the network be compromised?**
- A.** No. XMS resides outside the data path, so performance bottlenecks and points of failure are eliminated.
- Q. Why didn’t the maps I created appear the next time I logged in?**
- A.** You must always save your maps. Also, if you make changes and you want your changes to appear on all clients (not just your local machine) you must save the changes to the server.
- Q. Why can’t I access the BIOS screen when the system boots up? (XM-3300 only)**
- A.** You must have a PS/2 keyboard attached to the XM-3300 to access the BIOS screen. A USB keyboard is dependent on Windows and only becomes effective after the Windows environment has loaded.

Contact Information

Xirrus, Inc. is located in Thousand Oaks, California, just 55 minutes northwest of downtown Los Angeles and 40 minutes southeast of Santa Barbara.

Xirrus, Inc.

2101 Corporate Center Drive

Thousand Oaks, CA 91320

USA

Tel: 1.805.262.1600

1.800.947.7871 Toll Free in the US

Fax: 1.866.462.3980

www.xirrus.com

support.xirrus.com

Page is intentionally blank

Glossary of Terms

802.11a

A supplement to the IEEE 802.11 WLAN specification that describes radio transmissions at a frequency of 5 GHz and data rates of up to 54 Mbps.

802.11b

A supplement to the IEEE 802.11 WLAN specification that describes radio transmissions at a frequency of 2.4 GHz and data rates of up to 11 Mbps.

802.11g

A supplement to the IEEE 802.11 WLAN specification that describes radio transmissions at a frequency of 2.4 GHz and data rates of up to 54 Mbps.

802.11n

A supplement to the IEEE 802.11 WLAN specification that describes enhancements to 802.11a/b/g to greatly enhance reach, speed, and capacity.

Alarm

An alarm results from the correlation of events and represents a failure or fault in the network that may need immediate attention.

Application Client

An applet that resides on the local machine where the XMS server resides that provides access to the client interface.

Array

A Xirrus proprietary high capacity wireless access point utilizing Gigabit LAN speeds and multiple wireless channels, specifically designed for the Enterprise market. See also, [XN16/XN12/XN8/XN4](#), [XS16/XS12/XS8/XS4](#), [XS-3900/XS-3700/XS-3500](#).

Authentication

The process that a station, device, or user employs to announce its identity to the network which validates it. IEEE 802.11 specifies two forms of authentication, open system and shared key.

Bandwidth

Specifies the amount of the frequency spectrum that is usable for data transfer. In other words, it identifies the maximum data rate a signal can attain on the medium without encountering significant attenuation (loss of power).

Browser Client

A Java-based applet that provides remote access to the XMS client interface from a Web browser.

BSS

(Basic Service Set) When a WLAN is operating in infrastructure mode, each access point and its connected devices are called the Basic Service Set.

BSSID

The unique identifier for an access point in a BSS network. See also, **SSID**.

Channel

A specific portion of the radio spectrum—the channels allotted to one of the wireless networking protocols. For example, 802.11b and 802.11g use 14 channels in the 2.4 GHz band, only 3 of which don't overlap (1, 6, and 11). In the 5 GHz band, 802.11a uses 8 channels for indoor use and 4 for outdoor use, none of which overlap.

CoS

(Class of Service) A category based on the type of user, type of application, or some other criteria that QoS systems can use to provide differentiated classes of service.

Default Policy

See Global Policy.

DHCP

(Dynamic Host Configuration Protocol) A method for dynamically assigning IP addresses to devices on a network. DHCP issues IP addresses automatically within a specified range to client devices when they are first powered up.

DNS

(Domain Name System) A system that maps meaningful domain names with complex numeric IP addresses. DNS is actually a separate network—if one DNS

server cannot translate a domain name, it will ask a second or third until a server is found with the correct IP address.

Encryption

Any procedure used in cryptography to translate data into a form that can be decrypted and read only by its intended receiver.

Gateway

The gateway in a network that a computer will use to access another network if a gateway is not specified for use. In a network using subnets, a default gateway is the router that forwards traffic to a destination outside of the subnet of the transmitting device.

Gigabit Ethernet

The newest version of Ethernet, with data transfer rates of 1 Gigabit (1,000 Mbps).

Global Policy

A Global Policy groups a set of policies that can be applied to Arrays in one shot. It is simply a convenience that allows you to apply a set of policies in one step, rather than one at a time. It simplifies Array management by defining a set of policies that set a desired Array configuration. Different global policies may be created for different configurations that you commonly use. Global Policies were previously called default policies.

Host Name

Each computer running TCP/IP (regardless of the operating system) has a host name—also known as a machine name. Host names are used by networking applications, such as Telnet, FTP, Web browsers, etc. In order to connect to a computer running the TCP/IP protocol using its host name, the host name must be resolved to an IP address. Host name resolution is typically done by the Domain Name System (DNS). Changing a computer's host name does not change its NetBIOS name. See also, [DNS](#) and [NetBIOS](#).

IAP

(Integrated Access Point) A configurable wireless module (radio) dedicated to the Xirrus Wi-Fi Array family of products. There are 16 IAPs embedded within the XN16, XS16, and XS-3900; 12 IAPs embedded within the XN12 and XS12; 8 IAPs embedded within the XN8, XS8, and XS-3700 Array; and 4 IAPs embedded within the XN4, XS4, and XS-3500 Array.

Icon

A graphical symbol used in the XMS client interface to represent objects, such as Arrays within a map, alarms and events. See also, **Map Symbol**.

Intrusion Detection System

A Xirrus proprietary application that scans and monitors the XMS database for intruders.

MAC Address

(Media Access Control Address) A 6-byte hexadecimal address assigned by a manufacturer to a device.

Managed Network

The network under management by XMS. This includes all the Arrays discovered by XMS, and all of their IAPs and the devices that are associated to them.

Map

A pictorial representation of your network or subnet. The background image for the default main map supplied with XMS is a global map of the world, but you can change the background image of any map at any time. For example, you may want to organize your maps to reflect a corporate organization based on functional areas, physical site layouts, or geographic areas.

Map Symbol

Also known simply as “symbols,” these are graphical representations of Arrays in the XMS client interface maps. The symbol for an Array is a pictorial image of the Xirrus Wi-Fi Array. See also, **Icon**.

Mbps

(Megabits per second) A standard measure for data transmission speeds (for example, the rate at which information travels over the Internet). 1 Mbps denotes one million bits per second.

MTBF

(Mean Time Between Failures) Used in reports, this shows the average time (in hours and minutes) between failures of an Array.

MTTR

(Mean Time To Repair) Used in reports, this shows the average time (in minutes) to restore functionality to the Array following a failure.

NetBIOS

(Network Basic Input Output System) All computers running the Windows® operating system have a NetBIOS name. The NetBIOS name is specified by the user when Windows® networking is installed and configured. In order to connect to a computer running TCP/IP via its NetBIOS name, the name must be resolved to an IP address. A computer's NetBIOS name is often the same as the computer's host name, because most users accept the default settings when installing their Windows® operating system.

Node

A defined element of the hierarchical **Tree**. For example, the configuration node is a parent node to all child nodes residing under it, such as security policy and network policy, etc.

NTP

(Network Time Protocol) An Internet standard protocol (built on top of TCP/IP) that ensures the accurate synchronization (to the millisecond) of computer clock times in a network of computers. Running as a continuous background client program on a computer, NTP sends periodic time requests to servers, obtaining server time stamps and using them to adjust the client's clock.

packet

Data sent over a network is broken down into many small pieces—packets—by the Transmission Control Protocol layer of TCP/IP. Each packet contains the address of its destination as well the data. Packets may be sent on any number of routes to their destination, where they are reassembled into the original data. This system is optimal for connectionless networks, such as the Internet, where there are no fixed connections between two locations.

Policy

A pre-defined set of parameters that can be applied to multiple Arrays managed by XMS simultaneously. Policies fall into categories (for example, security, administration, network, firmware, etc.).

Polling

The process of contacting a network, Array or group of Arrays and collecting statistical data about the device(s).

QoS

(Quality of Service) QoS can be used to describe any number of ways in which a network provider guarantees a service's performance, such as an average or minimum throughput rate.

RADIUS

(Remote Authentication Dial-In User Service) A client-server security protocol, developed to authenticate, authorize, and account for dial-up users. The RADIUS server stores user profiles, which include passwords and authorization attributes.

Remote DC Power System

An optional Xirrus proprietary product that provides distributed DC power to multiple Wi-Fi Arrays, eliminating the need to run dedicated AC power to each unit and facilitating backup power when connected via a UPS.

RMI

(Remote Method Invocation) A set of protocols developed by Sun's JavaSoft® division that enables Java objects to communicate remotely with other Java objects. RMI is a relatively simple protocol, but unlike more complex protocols, such as CORBA and DCOM, it works only with Java objects. The XMS client interface utilizes Java.

Rogue

Any wireless device that is visible on your network but not recognized. You have the option of defining all rogue devices as either Unknown, Known, or Approved. Based on your definition, you can deny or allow access to the network for any rogue device.

RSSI

(Received Signal Strength Indicator) A measure of the energy observed by an antenna when receiving a signal.

SNMP

(Simple Network Management Protocol) A standard protocol that regulates network management over the Internet.

SNTP

(Simple Network Time Protocol) A simplified version of NTP. SNTP can be used when the ultimate performance of the full NTP implementation described in RFC 1305 is not needed or justified.

SSID

(Service Set IDentifier) Every wireless network or network subset (such as a BSS) has a unique identifier called an SSID. Every device connected to that part of the network uses the same SSID to identify itself as part of the family—when it wants to gain access to the network or verify the origin of a data packet it is sending over the network. In short, it is the unique name shared among all devices in a WLAN.

Subnet mask

A mask used to determine what subnet an IP address belongs to. An IP address has two components: (1) the network address and (2) the host address. For example, consider the IP address 150.215.017.009. Assuming this is part of a Class B network, the first two numbers (150.215) represent the Class B network address, and the second two numbers (017.009) identify a particular host on this network.

Symbol

Refer to **Map Symbol** and **Icon**.

Syslog

(SYStem LOGging) A protocol that allows a machine to send event notification messages across IP networks to event message collectors, known as Syslog servers. Syslog messages are based on the User Datagram Protocol (UDP). They are received on UDP port 514 and cannot exceed 1,024 bytes in length (they have no minimum length). See also, **UDP**.

Threshold

A value that determines the minimum and maximum limit for collected data. If the collected data violates a defined threshold, the system reports the fault as needing attention.

Transmit Power

The amount of power used by a radio transceiver to send the signal out. Transmit power is generally measured in milliwatts, which you can convert to dBm.

UDP

(User Data Protocol) A connectionless protocol that works at the OSI transport layer. UDP provides datagram transport but does not acknowledge their receipt. UDP is the protocol used for processing Syslog messages. See also, [Syslog](#).

VLAN

(Virtual LAN) A group of devices that communicate as a single network, even though they are physically located on different LAN segments. Because VLANs are based on logical rather than physical connections, they are extremely flexible. A device that is moved to another location can remain on the same VLAN without any hardware reconfiguration.

Wi-Fi Array

A family of Xirrus proprietary high capacity wireless access points utilizing multiple channels, specifically designed for the Enterprise market. See also, [Array](#).

XN16/XN12/XN8/XN4, XS16/XS12/XS8/XS4, XS-3900/XS-3700/XS-3500

A family of Xirrus proprietary high capacity wireless access points utilizing Gigabit LAN speeds and multiple wireless channels, specifically designed for the Enterprise market. The XN16, XS16, and XS-3900 Wi-Fi Arrays have 16 Integrated Access Points (IAPs). The XN12 and XS12 Wi-Fi Arrays have 12 IAPs; the XN8, XS8, and XS-3700 Wi-Fi Arrays have 8 IAPs; and the XN4, XS4, and XS-3500 Wi-Fi Arrays have 4 IAPs.

Index

Numerics

10/100 Fast Ethernet 239, 241
4.9 GHz Public Safety Band 326
802.11a settings 317, 331
802.11b/g settings 317, 333
802.11h Beacon Support 326
802.11n
 bonding 313
802.11n settings 317

A

abg2/abgn2
 self-monitoring, loopback mode 323
about images 39
about this guide 3
 organization 3
active backup
 between Gigabit ports 245
adding a map 144
adding Arrays 87
adding networks 78
Address Resolution Protocol (ARP) 324
Admin 229
admin accounts 236
admin RADIUS 271, 284
admin RADIUS account
 if using Console port 285
administration
 broadcast message 500
 country of operation 496
administrator
 Windows login 25
Advanced Feature Sets 189
advanced functionality 10

AeroScout tags 257
AES 273
aggregate traffic
 between Gigabit ports 245
alarm window
 SNMP trap 107
alarms 107
 taking action 110
announcement
 see broadcast message 500
antenna 314
ARP filtering 324
arranging windows
 basic window operations
 tiling 55
Array
 license, deleting 197
 license, exporting 191
 license, importing 192
 license, pending 196
 license, updating 194
 licensing window 190
 shell logins, entering 80
 software update
 from Array window 185
Array groups policy 366
Array icon 158
Arrays 165
 adding 87
 Array groups (policy) 366
 assigning (applying) policies 185, 223
 assigning to a group 183
 auto-configuration of channels 181
 configuring 174
 connecting to 172
 deleting 89, 182
 enabling/disabling IAPs for multiple Arrays 180
 host name 170

- how identified 170
 - label 170
 - licenses, managing 189
 - locating on a map 187
 - managing 163
 - maps, adding to 147
 - maps, moving 149
 - maps, removing 149
 - maps, resizing icon 148
 - PoGE injector management 187
 - rebooting 187
 - refreshing 88, 187
 - removing from a map 182
 - searching 164
 - software version 173
 - viewing events and alarms 186
 - viewing reports 186
 - attributes of a policy 220
 - audit 370
 - authentication
 - Array shell logins 80
 - auto blocking, rogue APs 327
 - auto negotiate 242, 244
 - auto-channel
 - lock channel selection 313
 - auto-configuration
 - channels 181
 - automatic discovery 70
 - see discovery 74
- B**
- background images
 - changing, for maps 145
 - file name 160, 161
 - for maps 142
 - formats 143
 - physical size 143
 - resolution 143
 - backup
 - deleting from database 514
 - backup manager 52
 - backup, active
 - Gigabit ports 245
 - balance, load
 - between Gigabit ports 245
 - balancing, load 325
 - band association 291
 - bandwidth 30
 - bandwidth reports 388
 - basic table operations 57
 - navigating 59
 - page length 59
 - rearranging tables 62
 - refreshing tables 59
 - resizing tables 62
 - row details 62
 - sorting 60
 - specifying a range 60
 - basic window operations
 - arranging windows 55
 - cascading 55
 - closing windows 56
 - detaching windows 53
 - maximizing 54
 - minimizing 54
 - navigating 53
 - re-attaching 53
 - beacon interval 321
 - beacons
 - 802.11h 326
 - benefits 9
 - blocked devices 124
 - blocking 327
 - blocking, rogue APs 327
 - blocking, rogue APs, reports 422
 - bonding 313
 - bridge traffic
 - between Gigabit ports 245
 - broadcast 324
 - broadcast message 500

Broadcast Rates 322
Browser Client 29, 30
browser login 29
buttons 42

C

capacity 7
cascading windows 55
cautions 5
Cell
 sharp cells 326
cell size 314
centralized management 9
channel selections
 lock 313
channel usage
 report 416
channels 312
 auto-configuration 181
 country of operation 496
CHAP (Challenge-Handshake Authentication Protocol)
 Admin RADIUS settings 286
 web page redirect 293, 294
classifying rogue devices
 by manufacturer 125
client
 connecting to XMS server 542
 login password 32, 34
 Web Start Client 29
client interface 39
 logging in 29
client login 29
client work space 40
closing windows 56
colors, changing
 on contour map 156
community string (name)
 SNMP 81
config file

 editing 365, 472
 policy 362
configuration
 auto-configuration of channels 181
configuration file
 policy 362
configuration management 10
configuration windows 50
connecting to XMS server
 problems 542
console 229, 237
Console port
 login via 285
contact information 544
contour map
 changing colors 156
 see RF Heat Map 131
country of operation
 channel selection 496
country, setting 320
creating a map 144
CSV
 exporting Array licenses 191
 importing Array licenses 192
custom login
 for software image upload 356
 for WPR file upload 361

D

dashboard 91
database
 about 501
 backups, deleting 514
 repairing 533
database server
 and XMS server shutdown 532
database windows 52
date/time restrictions
 and interactions 307
DB operations 501

- default lease 268
- default password 26, 32, 34, 503
- default policy
 - see global policy 185, 223
- default user name 26, 32, 34, 503
- delete
 - Array licenses 197
 - database backups 514
- deleting a network 86
- deleting an Array 89
- desktop icon
 - Web Start Client 29
- detaching windows 53
- devices
 - blocking 124
- DHCP server 247, 265
- disabling/enabling IAPs for multiple Arrays 180
- discovering
 - Arrays 67
 - networks 67
- discovering networks and Arrays 37
- discovery 70
 - disable (exclude) networks 74
 - optimizing 74
 - schedule 74
 - SNMP v2, v3 81
 - SNMPv3 requires NTP 68, 509, 543
- discovery properties 74
- display units
 - maps 161
- distance (scale)
 - setting on map 146
- DNS server 247, 248
- DTIM period 322
- duplex 244

E

- EAP 274
- edit mode

- for maps 137
- enabling/disabling IAPs for multiple Arrays 180
- encryption 275
- Enterprise class 14
- environment properties
 - wall setting on map 151
- Excel file
 - exporting Array licenses 191
 - importing Array licenses 192
- executing a policy 221
- export
 - Array licenses 191

F

- family of products 1
- FAQs 542
- Fast Ethernet 239, 241
- features 9
 - about licensing 189
 - supported by license 189
- figures
 - list of xiii
- filter
 - ARP 324
- filter policy 348
- find - see searching 164
- firewall
 - and port usage 22
- floor plan 130
 - for map 142
- frequently asked questions 542

G

- Gigabit 1 240, 243
- Gigabit 2 241, 246
- gigabit ports
 - see also port mode 245
- global policy 179
 - apply to Array 185

- create from Array 223
- global settings 317, 319
- glossary of terms 545
- group limits and interactions 307
- group, user
 - WPR (web page redirect) 306
- groups
 - policy 366

H

- Heat Map (RF) 131
- heat maps
 - migrating older maps 142
- host name
 - Array 170
- HTTPS 231
- hutting 38, 507
- hyperlinks 6

I

- IAP settings 310
- IAPs 198
 - bonding 313
 - channel 312
 - enabling/disabling for multiple Arrays 180
 - searching 164
- icon 158
- icon, desktop
 - Web Start Client 29
- identifying an Array 170
- IEEE 802.11n
 - bonding 313
- image
 - physical size 143
- image file size
 - minimizing 142
- image formats 143
- image resolution 143
- image resolution, for map 143

- image, software
 - update from Array window 185
- images 39
- implementing Voice over Wi-Fi 259
- import
 - Array licenses 192
- injector
 - PoGE, management 187
- injectors (PoGE)
 - managing 211
- installation 21
- installation prerequisites 16
- installing software updates
 - XA-3300-CC 17
- interface 39
- internal login page
 - web page redirect, customize 299
- internal RADIUS server 279
- internal splash page
 - web page redirect, customize 299
- interval
 - keepalive trap 233
- introduction 1
- Intrusion Detection System (IDS) 38
- IP address 26, 32, 34, 503
- IP range 268

J

- Java 29, 30
- Java applet
 - loading 33, 34

K

- keepalive traps 233
- key features 9
- keyboard shortcuts 46, 65

L

- label

- for an Array 170
- lease 268
- LED blink behavior 341
- LED settings 318, 340
- license
 - and features 189
 - and upgrades 189
 - Array, deleting 197
 - Array, exporting 191
 - Array, importing 192
 - Array, managing 189
 - Array, pending 196
 - Array, updating 194
 - Array, window 190
 - XMS server 35
- limits
 - group 307
 - interactions 307
 - station 307
 - traffic 307
- list of figures [xiii](#)
- load balance traffic
 - between Gigabit ports 245
- Load Balancing 325
- locate
 - Array on a map 187
- location
 - Wi-Fi tags 257
- lock
 - channel selections 313
- logging in 29
- login 29
 - via Console port 285
 - windows, for XMS 25
- login page
 - web page redirect, customize 299
- logins, Array shell
 - entering 80
- long retry limit 321
- loopback mode 323

M

- MAC list 271, 281
- main viewing area 46
- managed network 71
- management
 - PoGE injector 187
- management capacity 7
- management interface 39
- management settings 228, 229
- managing Array licenses 189
- managing Arrays 158, 163
- managing policies 215
- manufacturer
 - classifying rogue devices by 125
- map
 - locate Array 187
 - RF Heat Map 131
- map window 48
- maps
 - about 129
 - adding a new map 144
 - Arrays
 - moving 149
 - removing 149
 - resizing icon 148
 - Arrays, adding 147
 - background image, changing 145
 - background images 142
 - contour map colors 156
 - deleting 157
 - display units 161
 - distance (setting scale) 146
 - edit mode 137
 - editable 144
 - environment properties
 - wall setting on map 151
 - floor plan 142
 - image name 160, 161
 - label 160
 - managing Arrays 158

- map window, about 132
- migrating to new release 142
- monitor mode 137
- properties, modifying 145
- renaming 145
- saving 145
- scale, setting 146
- wall settings 151
- working with 129
- maximizing windows 54
- menu bar 41
- message
 - broadcast 500
- migrating older maps 142
- minimizing image file sizes 142
- minimizing windows 54
- mirror traffic
 - between Gigabit ports 245
- mode, for maps
 - see maps 137
- modify
 - map properties 145
- modifying a network 84
- monitor mode
 - for maps 137
- monitoring 11, 105
 - alarms 107
 - taking action 110
 - audit 370
 - dashboard 91
 - network events 111
 - severity levels 110
 - syslog
 - event details 114
 - severity levels 113
 - syslog events 112
 - viewing by Array 105
- monitoring windows 47
- MTU size 243, 245
- MySQL

- port usage 19, 20

N

- navigating windows 53
- NetBIOS 397
- NetFlow server 252
- Netflow server 252, 257
- network events 111
- network monitoring 11, 105
 - dashboard 91
- network policy 239
- network reporting 11
- network topology 7, 8
- networks
 - adding 78
 - deleting 86
 - modifying 84
 - rediscovering 85
- new map 144
- notes 5
- NTP 247
 - required with SNMPv3 68, 509, 543
- NTP server 112, 247, 250

O

- operating country
 - channel selection 496
- optimization, VLAN 324
- organization of this guide 3
- other navigation tools
 - keyboard shortcuts 45
 - right-click menus 45
- overview 7

P

- page length 59
- PAP (Password Authentication Protocol)

- Admin RADIUS settings 286
 - web page redirect 292, 294
 - parity 238
 - password 26, 32, 34, 503
 - SNMPv3 81
 - Windows, for XMS 25
 - XSMT 38
 - patches
 - installing on XA-3300-CC 17
 - performance monitoring 10
 - phone home trap 233
 - PoE 415, 476, 477, 478, 482
 - PoGE 415, 476, 477, 478, 482
 - PoGE injector
 - management 187
 - policies 215
 - Array groups 366
 - attributes 220
 - config file 362
 - configuration file 362
 - deleting 222
 - executing 221
 - existing 221
 - filters 348
 - management control 228
 - managing 215
 - network 239
 - RF 316
 - security 270
 - server 247
 - software update
 - from Array window 185
 - SSID 287, 301
 - system information 225
 - user accounts 497
 - VLAN 259
 - WDS 342
 - policy
 - apply to Array 185, 223
 - default, see global policy 223
 - global
 - see global policy 185, 223
 - port mode
 - active backup 245
 - aggregate traffic 245
 - bridge traffic 245
 - load balance traffic 245
 - mirror traffic 245
 - transmit on both ports 245
 - port requirements 22
 - ports 19, 20
 - Power over Gigabit Ethernet (PoE) 2
 - Power over Gigabit Ethernet (PoGE)
 - injectors
 - managing 211
 - prerequisites 16
 - product family 1
 - product overview 7
 - properties
 - map, modifying 145
 - PSK 273
 - public safety band 326
- ## Q
- QoS 291
 - queue
 - report 383
 - quick reference guide
 - keyboard shortcuts 65
- ## R
- RADIUS 271, 276
 - admin RADIUS 284
 - Array logins 80
 - external 277
 - internal 277, 279
 - RADIUS settings
 - web page redirect 292, 294
 - RADIUS, admin 271
 - admin RADIUS 285

- rearranging tables 62
- re-attaching windows 53
- rediscovering networks 85
- refreshing an Array 88
- refreshing tables 59
- remote login 29
- renaming
 - maps 145
- repairing database 533
- report
 - queue 383
- reporting 11
- reports 371
 - about 371
 - Array availability 412
 - bandwidth 388
 - by Array speed 389, 392, 402
 - by Array utilization 416, 419
 - by station speed 394
 - error
 - by station 397
 - list of 371
 - main window 373
 - RF 416
 - schedule
 - specific date range 382, 383
 - security 419
 - rogue list 420
 - station
 - by Array 406
 - by station 405
 - station association 404
 - viewing from Array window 186
- resizing tables 62
- resource window
 - searching 164
- resources
 - managing PoGE injectors 211
- resources windows 48
- restrictions

- date/time 307
- stations 307
- traffic 307
- RF
 - sharp cells 326
- RF Heat Map 131
- RF policy 316
 - global, load balancing 325
- RF reports 416
- RFID tags 257
- right-click menus 45
- rogue APs
 - blocking, reports 422
- rogue devices
 - classifying by manufacturer 125
- rogues 327
 - clocking 124
- runtime 33, 34

S

- save
 - maps 145
- scalability 9
- scale, setting
 - for map 146
- schedule
 - discovery 74
- scheduling the discovery process 74
- searching 64
 - in devices window 164
 - in resource windows 164
- Secure Channel Protocol (SCP) 356, 361
- security 270, 272
- security management 9
- security policy 270
- security reports 419
- security settings 272
- security windows 50
- self-monitoring

- options 323
 - serial interface 237
 - server
 - database
 - repairing 533
 - login 531
 - port assignments 531
 - shut down 531
 - server console 27, 524
 - server policy 247
 - server, VTun
 - see VTun 263
 - service
 - XMS server as Windows service 523
 - severity levels 110, 113
 - Sharp cells 326
 - shell
 - Array login, entering 80
 - short retry limit 321
 - shutting down the unit 38, 507
 - shutting down the XM-3300 507
 - shutting down XMS server 38
 - SNMP 87
 - discovery 81
 - port usage 19, 20
 - v2 81
 - v3 81
 - SNMP server 232, 234, 247
 - SNMP trap
 - shown on Alarm window 107
 - SNMPv3
 - NTP usage required 68, 509, 543
 - time sync with Arrays 68, 509, 543
 - software
 - update Array image
 - from Array window 185
 - software update
 - SSH port 518, 539
 - software updates
 - installing on XA-3300-CC 17
 - software version, running on the Array 173
 - sorting tables 60
 - client level 60
 - server level 60
 - splash page
 - web page redirect, customize 299
 - SSH 230
 - port for software updates 518, 539
 - SSID 207
 - WPR (web page redirect) 291
 - SSID list 289
 - SSID policy 287, 301
 - Standby 248
 - starting client
 - starting Web Start Client 29
 - station association reports 404
 - stations 203, 323
 - blocking 325
 - inactivity time out 322
 - limits and interactions 307
 - reauthentication 322
 - searching 164
 - status bar 44
 - status message 44
 - stop bits 238
 - stopping the server 38, 507
 - syslog
 - event details 114
 - port usage 19, 20
 - services policy 253
 - syslog events 112
 - syslog server 112, 247, 253
 - System 248
 - system log
 - see syslog 253
- T**
- table rows 62

- tags, Wi-Fi 257
- TCP
 - port requirements 22
- technical support 541
 - contact information 544
 - frequently asked questions 542
- Telnet 230
- testing
 - loopback mode 323
- threshold settings 332, 335
- tiling windows 55
- TKIP 273
- tool tips 44
- toolbar 42
 - buttons 42
- topography 129
- topology 7, 8
- traffic
 - aggregate Gigabit ports 245
 - bridge Gigabit ports 245
 - limits and interactions 307
 - load balance Gigabit ports 245
 - mirror Gigabit ports 245
 - transmit on both Gigabit ports 245
- trap
 - keepalive 233
 - phone home 233
- tree 43
- Tunnel Port 263
- Tunnel Secret 263
- tunnel server 263
- tunnels
 - see VTun 263

U

- UDP
 - port requirements 22
- update
 - software, from Array window 185
- updates

- software, installing on XA-3300-CC 17
- upgrade
 - about licensing 189
- upgrade packs 7
- upload to Array
 - custom login 356, 361
- used by XMS server 19, 20
- user accounts policy 497
- user group
 - WPR (web page redirect) 306
- user group limits and interactions 307
- user interface 39
- user name 26, 32, 34, 503
- username
 - SNMPv3 81

V

- version, software running on the Array 173
- viewing
 - discovered Arrays 72
 - discovered networks 72
- virtual tunnels
 - see VTun 263
- VLAN
 - broadcast optimization 324
- VLAN ID 291, 304
- VLAN policy 259
- voice
 - implementing on Array 259
- VTs
 - Virtual Tunnel Server 263
- VTUN 259, 263
- VTun
 - specifying tunnel server 263

W

- wall setting
 - for map 151

- WDS policy 342
- Web Management Interface
 - opening for Array 172, 180
 - starting for an Array 200, 205
- web page redirect
 - CHAP (Challenge-Handshake Authentication Protocol) 293, 294
 - customize internal login/splash page 299
 - PAP, CHAP 292, 294
 - RADIUS settings 292, 294
 - see WPR 358
- Web Page Redirect (WPR) 358, 362
- Web Start Client 29
- WEP 274
- Wi-Fi tags 257
- window
 - Array licensing 190
- Windows
 - login 25
- Windows server
 - shutting down 38, 507
- Windows service 523
- WLAN management 320
- word size 238
- work space
 - backup manager 52
 - configuration windows 50
 - main viewing area 46
 - major components 40
 - map window 48
 - menu bar 41
 - monitoring windows 47
 - resources windows 48
 - security window 50
 - status bar 44
 - tool tips 44
 - toolbar 42
 - tree 43
- WPA 273
- WPR
 - in SSIDs 291
 - in user groups 306
 - policy (uploading WPR files) 358
- X**
- XA-3300-CC
 - installing software updates 17
- Xirrus Advanced Feature Sets 189
- Xirrus Server Management Tool
 - see XSMT 38
- Xirrus XP Power System 2
- XM-3300 1
 - (Xirrus Management Platform) 1
 - shutting down 38, 507
 - stopping the server 38, 507
- XMS
 - managed network 71
 - port requirements 22
 - server license 35
- XMS client
 - connecting to XMS server 542
- XMS server
 - as Windows service 523
 - license 35
 - managing - see XSMT 38
 - port usage 19, 20
 - problems connecting client 542
 - shutting down 38
- XMS server login 25
- XMS user accounts 497
- XP1 Power over Gigabit Ethernet (PoE) 2
- XP-3100 2
- XS16 2
- XS-3500 2
- XS-3700 2
- XS-3900 2
- XS4 2

XS8 [2](#)

XSMT

password [38](#)

shutdown XMS server [38](#)

Xirrus Server Management Tool [38](#)

User's Guide



Xirrus Management System